Dr.WEB®

Agent für Windows

Defend what you create

Benutzerhandbuch

© Doctor Web, 2015. Alle Rechte vorbehalten

Das im vorliegenden Dokument enthaltene Material ist Eigentum von Doctor Web und dient ausschließlich der persönlichen Nutzung durch Produktkäufer. Kein Teil des vorliegenden Dokumentes darf ohne Quellenangabe weder reproduziert noch auf einer Netzwerkressource untergebracht oder mittels Kommunikationskanäle und Massenmedien verbreitet oder auf jede andere Weise benutzt werden, ausgenommen Nutzung für persönliche Zwecke.

WARENZEICHEN

Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, Dr.Web AV-Desk, Dr.WEB Logos sind eingetragene Warenzeichen von Doctor Web in Russland und/oder anderen Ländern. Alle sonstigen eingetragenen Warenzeichen, Logos und Firmennamen, die im vorliegenden Dokument erwähnt sind, sind Eigentum ihrer jeweiligen Inhaber.

HAFTUNGSAUSSCHLUSS

Unter keinen Umständen haften Doctor Web und seine Lieferanten für die im vorliegenden Dokument enthaltenen Fehler und/oder Auslassungen sowie für Schäden des Produktkäufers (direkte oder indirekte Schäden einschließlich Gewinnausfälle), die sich dadurch ergeben.

Dr.Web Agent
Version 10.0
Benutzerhandbuch
28.07.2015

Doctor Web, Hauptsitz Russland
Tretja ul. Jamskogo polja 2, Gebäude 12A
125124 Moskau
Russische Föderation

Website: www.drweb.com
Telefon: +7 (495) 789-45-87

Nähere Informationen zu den regionalen Vertretungen und Büros finden Sie auf unserer Website

Doctor Web

Doctor Web ist ein russischer Anbieter hauseigener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antivirus- und Antispam-Lösungen sowohl für staatliche Einrichtungen und große Unternehmen als auch für private Benutzer.

Die Antivirensoftware von Dr.Web wird seit 1992 entwickelt. Die Antivirus-Lösungen zeigen immer wieder hervorragende Leistungen bei Entdeckung von Malware und entsprechen den weltweiten Sicherheitsnormen.

Zertifikate und Auszeichnungen sowie umfangreiche Geographie der Benutzer zeugen vom besonderen Vertrauen der Kunden in unsere Produkte.

Wir danken den Benutzern für Unterstützung der Lösungen von Dr.Web-Familie!

Inhaltsverzeichnis

1. Einleitung 6

1.1. Über dieses Handbuch 7

1.2. Symbole und Abkürzungen 7

1.3. Entdeckungsverfahren 8

2. Systemanforderungen 10

3. Programm installieren, ändern oder deinstallieren 12

3.1. Installation mithilfe eines vollständigen Installationspakets 12

3.2. Installation mithilfe eines Installationspakets der Lite-Version 18

3.3. Programm ändern bzw. deinstallieren 25

4. Erste Schritte 27

4.1. Antivirus überprüfen 30

5. Tools 31

5.1. Quarantänemanager 31

5.2. Support 32

5.2.1. Bericht erstellen 33

6. Dr.Web Scanner 34

6.1. Suchlauf starten 34

6.2. Aktionen bei Bedrohungserkennung 37

6.3. Scanner konfigurieren 38

6.4. Scanner mit Befehlszeilenparametern starten 45

6.5. Konsolen-Scanner 46

6.6. Überprüfung nach Zeitplan starten 46

7. Einstellungen 48

8. Allgemeine Einstellungen 49

8.1. Benachrichtigungen 49

8.2. Selbstschutz 51

8.3. Endgeräte 52

8.4. Erweitert 53

8.5. Modus 56

9. Office Control 59

9.1. Office Control konfigurieren 60

10. Ausnahmen 62

10.1. Webseiten 62
10.2. Dateien und Verzeichnisse schützen 62
10.3. Programme und Prozesse 63
10.4. Antispam 64
11. Schutzkomponente 65
11.1. SpIDer Guard 65
11.1.1. SpIDer Guard konfigurieren 65
11.2. SpIDer Gate 69
11.2.1. SpIDer Gate konfigurieren 69
11.3. SpIDer Mail 71
11.3.1. SpIDer Mail konfigurieren 72
11.4. Antispam 75
11.5. Dr.Web Firewall 77
11.5.1. Dr.Web Firewall Trainingsmodus 77
11.5.2. Firewall konfigurieren 79
11.6. Dr.Web für Outlook 87
11.6.1. Dr.Web für Outlook einstellen 87
11.6.2. Erkennung von Bedrohungen 88
11.6.3. Spam-Prüfung 91
11.6.4. Ereignisse protokollieren 95
11.6.5. Scanstatistiken 96
11.7. Präventivschutz 96
Anhänge 100
Anhang A. Befehlszeilenparameter 100
Befehlszeilenparameter für Scanner und Konsolen-Scanner 100
Befehlszeilenparameter für Installationspakete 104
Rückgabecodes 106
Anhang B. Bedrohungen und ihre Neutralisierung 107
Klassifizierung von Bedrohungen 107
Neutralisierung von Bedrohungen 111
Anhang C. Benennung von Bedrohungen 112
Schlagwortregister 0

1. Einleitung

Dr.Web Agent bietet mehrstufigen Schutz für den Systemspeicher, Festplatten und Wechseldatenträger vor beliebigen Viren, Rootkits, Trojanern, Spy- und Adware, Hacktools und allen möglichen Typen der schädlichen Objekte aus beliebigen äußeren Quellen.

Das Programm **Dr.Web** zeichnet sich durch eine bequeme Modularchitektur aus. **Dr.Web** verwenden eigene Antivirus-Engine und Virendatenbanken, die für alle Komponenten und Betriebssysteme gemeinsam sind. Neben **Dr.Web** sind heutzutage verfügbar auch Versionen für IBM® OS/2®, Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Android®, Symbian® sowie für die Familie von Unix® (z. B. Linux®, FreeBSD® und Solaris®).

Dr.Web verwendet einen bequemen und effektiven Verfahren zur Aktualisierung der Virendatenbanken und Komponenten des Programms über das Internet.

Dr.Web erkennt und entfernt verschiedene unerwünschte Programme (Adware, Dialer, Scherzprogramme, Riskware, Hacktools). Zur Erkennung von unerwünschten Programmen und Ausführung der Aktionen für die in diesen Programmen enthaltenen Dateien werden die jeweiligen Komponenten von **Dr.Web** verwendet.

Jede **Dr.Web** Sicherheitslösung für Betriebssysteme von Microsoft® Windows® enthält jeweils die folgenden Komponenten:

Dr.Web Scanner ist ein Scanner mit der Benutzeroberfläche, der auf Anforderung des Benutzers gestartet wird und den Rechner auf Viren überprüft.

Dr.Web Konsolen-Scanner ist eine Version des **Dr.Web Scanners** mit der Befehlszeilenschnittstelle.

SpIDer Guard ist ein speicherresidenter Antivirus-Wächter, der Dateien und laufende Prozesse in Echtzeit scannt und das System vor verdächtigen und bösartigen Aktivitäten schützt.

SpIDer Mail ist ein E-Mail-Wächter, der Zugriffe von laufenden E-Mail-Clients auf Mailserver überwacht. Dabei wird der Datenverkehr über die Protokolle POP3/SMTP/IMAP4(IMAPv4rev1)/NNTP überprüft. Dadurch werden E-Mail-Viren erkannt und desinfiziert, bevor der E-Mail-Client infizierte E-Mails vom Server empfängt oder eine E-Mail an Server gesendet wird. Der E-Mail-Wächter kann auch E-Mails mithilfe von **Dr.Web Antispam** auf Spam überprüfen.

Dr.Web für Outlook ist ein Plug-In. Es überprüft E-Mail-Postfächer von Microsoft Outlook auf Viren und Spam.

SpIDer Gate – HTTP-Wächter. Standardmäßig prüft **SpIDer Gate** automatisch den eingehenden HTTP-Traffic und blockiert die Übermittlung von Objekten, die Viren und sonstige Malware enthalten. Standardmäßig ist auch die URL-Filterung der nicht empfohlenen Websites sowie der als Virenverteiler bekannten Websites aktiviert.

Office Control – diese Komponente schränkt den Zugriff auf bestimmte Webseiten, Dateien und Ordner ein und kontrolliert die im Internet oder am Rechner verbrachte Zeit.

Dr.Web Firewall ist eine persönliche Firewall, die Ihren Rechner vor ungewolltem Zugriff von außen schützt und dem Datenverlust im Netzwerk vorbeugt.

SpIDer Agent ist ein Verwaltungsmodul, mit dem Sie Komponenten von **Dr.Web** starten und konfigurieren können.

1.1. Über dieses Handbuch

Das Handbuch beschreibt die Installation und Bedienung des Programms **Dr.Web**.

Die detaillierte Beschreibung aller Elemente der grafischen Benutzeroberfläche finden Sie in der Hilfedatei, die in jeder Komponente des Programms aufgerufen werden kann.

Dieses Handbuch liefert Ihnen detaillierte Hinweise zur richtigen Installation und Bedienung des Programms sowie zur erfolgreichen Virenabwehr. Das Handbuch beschreibt meistens die standardmäßige Verwendung der Komponenten (mit Standardeinstellungen) von **Dr.Web**.

In Anhängen finden Sie weitere hilfreiche Informationen zum Verwalten von **Dr.Web**, die aber ausschließlich für erfahrene Benutzer oder Servicetechniker bestimmt sind .

Da unsere Produkte kontinuierlich weiterentwickelt werden, können einige Elemente der Oberfläche von den in diesem Handbuch abgebildeten/beschriebenen Elementen leicht abweichen. Die aktuellsten Hilfeinformationen finden Sie immer unter http://download.drweb-av.de/doc?lng=de.

1.2. Symbole und Abkürzungen

In diesem Handbuch werden die folgenden Symbole und Hervorhebungen verwendet.

Symbol/Hervorhebung	Erläuterung
Fette Schrift	Elemente der grafischen Benutzeroberfläche und Beispiele für Eingaben, die man exakt durchführen muss, wie sie in der Anleitung stehen.
Grüne fette Schrift	Namen der Produkte von **Doctor Web** bzw. deren Komponenten.
Fette unterstrichene Schrift	Querverweise auf andere Seiten im Handbuch oder auf Webseiten.
`Festbreitenschrift`	Beispiele für Code, Eingaben in der Befehlszeile und Informationen, die der Benutzer von der Anwendung erhält.
Kursivschrift	Begriffe und Platzhalter (wird anstelle von Informationen verwendet, die vom Benutzer eingegeben werden müssen). Bei Eingaben in der Befehlszeile deutet die kursive Schriftart auf Parameterwerte hin.
GROSSBUCHSTABEN	Namen der Tastatur-Tasten.
Pluszeichen („+“)	Tastenkombination. Zum Beispiel, die Kombination ALT+F1 bedeutet, dass die Taste F1 gedrückt werden muss, indem die Taste ALT gedrückt gehalten wird.
Ausrufezeichen	Wichtiger Hinweis bzw. Warnung vor potentiell gefährlichen oder fehleranfälligen Situationen.

1.3. Entdeckungsverfahren

Alle Antivirusprogramme von **Doctor Web** setzen gleichzeitig mehrere Entdeckungsverfahren von schädlichen Objekten ein. Dies ermöglicht es, dass alle verdächtigen Dateien maximal sorgfältig durchsucht werden.

Entdeckungsverfahren von Bedrohungen

Signaturanalyse

Dieses Verfahren wird in erster Linie eingesetzt. Es basiert auf der Prüfung vom Inhalt des zu analysierenden Objekts. Es wird dabei festgestellt, ob die Signaturen der bereits bekannten Bedrohungen darin enthalten sind.*Signatur* ist eine kontinuierliche endliche Byte-Reihenfolge, die einzigartig für eine bestimmte Computerbedrohung definiert ist. Dabei wird der Inhalt des analysierten Objektes mit Signaturen nicht direkt, sondern anhand von deren Kontrollsummen verglichen. Dadurch wird die Größe der Einträge in den Virendatenbanken wesentlich verringert. Die Übereinstimmung bleibt aber dabei eindeutig, die Bedrohungen werden korrekt erkannt und infizierte Objekte werden korrekt desinfiziert. **Dr.Web Virendatenbanken** sind so zusammengesetzt, dass mehrere Klassen und Familien von Bedrohungen nur mit einer Signatur entdeckt werden können.

Origins Tracing™

Es ist eine einzigartige Technologie von **Dr.Web**, die zur Entdeckung von neuen und modifizierten Bedrohungen dient, die bereits bekannte und in den Virendatenbanken beschriebene Infizierungsmechanismen oder schädliches Verhalten benutzen. Dieses Verfahren wird nach Abschluss der Signaturanalyse durchgeführt und schützt die Benutzer der Antivirus-Lösungen von **Dr.Web** vor solchen Bedrohungen, wie z.B. Trojan.Encoder.18 (der auch unter dem Namen „gpcode" bekannt ist). Weiterhin ermöglicht es **Origins Tracing**, die Anzahl der Fehlauslösungen von der heuristischen Analyse zu reduzieren. Zu den Namen von Bedrohungen, die mit Hilfe von **Origins Tracing** erkannt werden, wird die Endung `.Origin` hinzugefügt.

Emulation

Die Emulationsmethode zur Ausführung des Programmcodes wird zur Entdeckung von polymorphen und verschlüsselten Viren eingesetzt, wenn die Suche nach Kontrollsummen von Signaturen unmöglich oder wesentlich komplizierter ist als die Erstellung zuverlässiger Signaturen. Das Verfahren basiert sich auf Imitation der Ausführung des zu analysierenden Codes durch den *Emulator* - ein Simulationsmodell des Prozessors und der Ablaufumgebung. Der Emulator operiert mit einem geschützten Speicherbereich *(Emulationsbuffer*). Dabei werden die Anweisungen zur Ausführung dem zentralen Prozessor nicht übermittelt. Wenn der durch den Emulator behandelte Code infiziert ist, wird der ursprüngliche schädliche Code wiederhergestellt, der für die Signaturanalyse geeignet ist.

Heuristische Analyse

Das Prinzip der heuristischen Analyse basiert auf einem Satz von *Heuristiken* (Vermutungen, deren statistische Signifikanz empirisch bewiesen ist) über kennzeichnende Merkmale eines schädlichen sowie eines zuverlässigen ausführbaren Codes. Jedes Merkmal besitzt einen bestimmten Punktwert (eine Zahl, die Wichtigkeit und Zuverlässigkeit dieses Merkmales anzeigt). Der Punktwert kann positiv sein, wenn das Merkmal auf schädliches Verhalten des Codes hindeutet. Der Punktwert ist negativ, wenn das Merkmal für die Computerbedrohungen nicht kennzeichnend ist. Aufgrund des Gesamtwertes, der den Inhalt des Objektes kennzeichnet, wird die Wahrscheinlichkeit des Vorhandenseins eines unbekannten schädlichen Objektes darin mittels der heuristischen Analyse festgestellt. Wenn diese Wahrscheinlichkeit einen bestimmten Grenzwert übersteigt, wird es festgestellt, dass das analysierte Objekt schädlich ist.

Bei der heuristischen Analyse wird auch die Technologie **FLY-CODE™** verwendet. Es ist ein allgemein einsetzbarer Algorithmus zur Entpackung von Dateien. Dieses Verfahren ermöglicht es, die heuristischen Vermutungen über das Vorhandensein der schädlichen Objekte in Objekten, die mit einem Packprogramm komprimiert wurden, anzustellen. Es handelt sich dabei nicht nur um Packprogramme, die den **Dr.Web**-Softwareentwicklern bekannt sind, sondern auch um neue Programme, die noch nicht erforscht sind. Bei der Durchsuchung der verpackten Objekte wird auch das Verfahren zur Analyse ihrer Strukturentropie eingesetzt. Diese Technologie erlaubt es, die Bedrohungen nach strukturellen Besonderheiten ihres Codes zu entdecken. Mit dieser Technologie können unterschiedliche Bedrohungen, die mit dem gleichen polymorphen Packer gepackt wurden, anhand von einem Eintrag in der Virendatenbank erkannt werden.

Da die heuristische Analyse ein System zur Hypothesenprüfung unter Unbestimmtheitsbedingungen ist, können dabei Fehler sowohl der ersten (Nichterkennen der unbekannten Bedrohungen) als auch der zweiten Art (ein sicheres Programm wird als ein Schadprogramm beurteilt) auftreten. In diesem Zusammenhang erhalten die bei der heuristischen Analyse als „schädlich" markierten Objekte den Status „verdächtig".

Bei einer beliebigen Prüfung werden die aktuellsten Informationen über bekannte Schadprogramme von allen **Dr.Web** Antivirus-Komponenten verwendet. Die Virensignaturen, die Informationen über ihre Merkmale und Verhaltensmodelle werden sofort aktualisiert und den Virendatenbanken hinzugefügt, wenn Experten aus dem **Virenlabor von Doctor Web** neue Bedrohungen entdecken, manchmal kann es mehrmals pro Stunde passieren. Selbst wenn das neueste Schadprogramm trotz des residenten Schutzes von **Dr.Web** in den Computer eindringt, wird dieses in der Prozessliste angezeigt und nach der Aktualisierung der Virendatenbanken neutralisiert.

2. Systemanforderungen

Vor der Installation von **Dr.Web** müssen Sie die folgenden Aktionen durchführen:

- Sämtliche installierten Antivirenprogramme von Ihrem Rechner entfernen, um die Inkompatibilität mit residenten Komponenten von **Dr.Web** zu vermeiden.
- Bei der Installation von **Firewall** ist es erforderlich, andere Firewalls zu deinstallieren.
- Alle vom Hersteller Ihres Betriebssystems empfohlenen kritischen Updates installieren. Falls Ihr Betriebssystem nicht mehr unterstützt wird, empfehlen wir Ihnen, auf ein neueres Betriebssystem umzusteigen.

Die nachfolgenden Bedingungen müssen erfüllt werden, damit **Dr.Web** betrieben werden kann.

Komponente	Anforderungen
Prozessor	Vollständige Unterstützung des Befehlssystems i686.
Betriebssystem	Für 32-Bit- Versionen der Betriebssysteme: • Windows XP mit Service Pack 2 oder höher; • Windows Vista mit Service Pack 2 oder höher; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10; • Windows Server 2003 mit Service Pack 1; • Windows Server 2008 mit Service Pack 2 oder höher. Für 64-Bit-Versionen der Betriebssysteme: • Windows Vista mit Service Pack 2 oder höher; • Windows 7; • Windows 8; • Windows 8.1; • Windows 10; • Windows Server 2008 mit Service Pack 2 oder höher; • Windows Server 2008 R2; • Windows Server 2012; • Windows Server 2012 R2. Bei der Installation können Microsoft Updates für Systemkomponenten eventuell heruntergeladen und installiert werden. In diesem Fall teilt **Dr.Web** Ihnen ihre Namen sowie Links zum Herunterladen mit.
Freier Arbeitsspeicher	Mindestens 512 MB.
HDD	1 GB für Antivirus-Komponenten. Dateien, die bei der Installation erstellt werden, benötigen zusätzlichen Speicherplatz.
Auflösung	Die empfohlene Bildschirmauflösung: mindestens 800x600 Pixel.
Sonstiges	Zur Aktualisierung von **Dr.Web Virendatenbanken** und Komponenten von **Dr.Web** ist eine Verbindung mit dem zentral verwalteten Virenschutz-Server oder Internet im Mobilmodus erforderlich. Um **Dr.Web für Outlook** verwenden zu können, brauchen Sie einen installierten E-Mail-Client Microsoft Outlook vom MS Office-Paket: • Outlook 2000 (Outlook 9), • Outlook 2002 (Outlook 10 oder Outlook XP),

Komponente	Anforderungen
	• Office Outlook 2003 (Outlook 11), • Office Outlook 2007, • Office Outlook 2010, • Office Outlook 2013.

Dr.Web Agent ist inkompatibel mit Plug-Ins **Dr.Web für Microsoft Exchange Server**, **Dr.Web für IBM Lotus Domino**, **Dr.Web für Kerio WinRoute**, **Dr.Web für Kerio MailServer**, **Dr.Web für Microsoft ISA Server und Forefront TMG**, **Dr.Web für Qbik WinGate** Version 6.0 und älter.

Weitere Konfigurationsanforderungen entsprechen den Konfigurationsanforderungen jeweiliger Betriebssysteme.

3. Programm installieren, ändern oder deinstallieren

Vor Installationsbeginn von **Dr.Web** geben Sie Acht auf die Systemanforderungen. Außerdem empfehlen wir Ihnen ausdrücklich, Folgendes durchzuführen:

- alle kritischen Microsoft-Updates für Ihre Version des Betriebssystems herunterzuladen (diese Updates können von der Microsoft-Webseite unter http://windowsupdate.microsoft.com heruntergeladen und installiert werden);
- das Dateisystem mit Hilfe von systemeigenen Mitteln überprüfen und gefundene Fehler beheben;
- laufende Anwendungen schließen.

Vor Installationsbeginn entfernen Sie von Ihrem Rechner andere Antivirensoftware und Firewalls, um mögliche Inkompatibilität zwischen residenten Komponenten zu vermeiden.

Sie können **Dr.Web** auf zwei Weisen installieren, ändern oder deinstallieren:

1. Per Fernzugriff – im Netzwerk über zentral verwalteten Virenschutz-Server. Dies wird vom Administrator des Antivirus-Netzwerks ohne Eingriff seitens Benutzers durchgeführt.
2. Lokal – direkt auf dem PC des Benutzers. Dabei kann entweder Komplettes Installationspaket oder seine Lite-Version zur Installation von **Dr.Web** verwendet werden.

3.1. Installation mithilfe eines vollständigen Installationspakets

Um **Dr.Web** zu installieren, benötigen Sie die Administratorrechte.

Die Installation von **Dr.Web** kann in jedem der folgenden Modi durchgeführt werden:

- im Hintergrundmodus;
- im üblichen Modus.

Installation über Befehlszeile

Um die Installation von **Dr.Web** über die Befehlszeile zu starten, geben Sie in der Befehlszeile erforderliche Parameter an. Beim Starten des folgenden Befehls wird beispielsweise **Dr.Web** im Hintergrundmodus installiert:

```
drweb-esuite-agent-full-10.00.0-xxxxxxxxx-windows.exe /silent yes
```

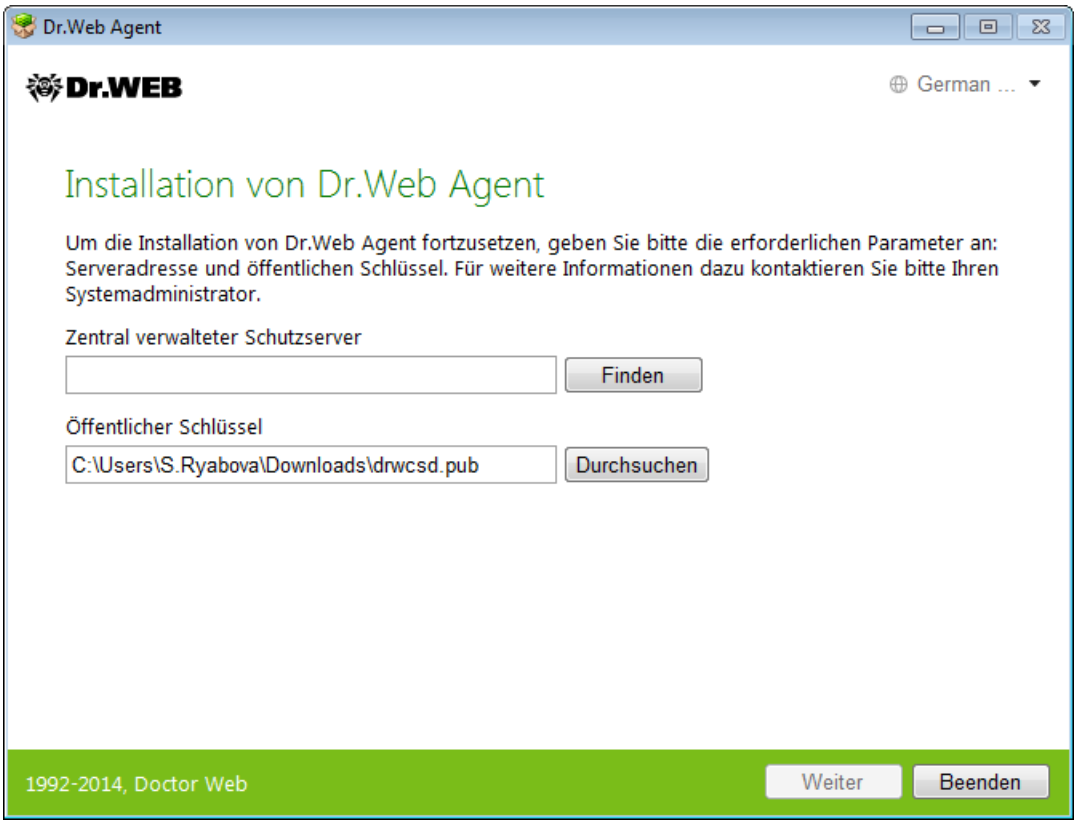
Alle verfügbaren Befehlszeilenparameter für Installationspakete finden Sie im Anhang A.

Installation im üblichen Modus

1. Starten Sie das Installationspaket, das Sie vom Administrator erhalten haben.

Wurden andere Antivirusprogramme auf der Workstation bereits installiert, versucht der Installations-Assistent diese zu entfernen.Sollte die Deinstallation fehlgeschlagen sein, müssen Sie die auf der Workstation benutzte Antivirensoftware selbständig entfernen.

Es öffnet sich das Dialogfeld des Installations-Assistenten von **Dr.Web**.



2. Im Feld **Zentral verwalteter Virenschutz-Server** wird die Netzwerkadresse des Servers angegeben, von **Dr.Web** installiert wird. Im Feld **Öffentlicher Verschlüsselungsschlüssel** wird der vollständige Pfad des öffentlichen Verschlüsselungsschlüssels (drwcsd.pub) auf Ihrem Computer angegeben.

   Klicken Sie auf **Weiter.** Es wird das Verfahren zur Herstellung der Verbindung zum Server gestartet.

   Wenn keine Verbindung hergestellt wurde, folgen Sie dem Link und überprüfen Sie die Netzwerkparameter und/oder versuchen Sie den Verbindungsversuch erneut, indem Sie auf entsprechenden Button klicken.

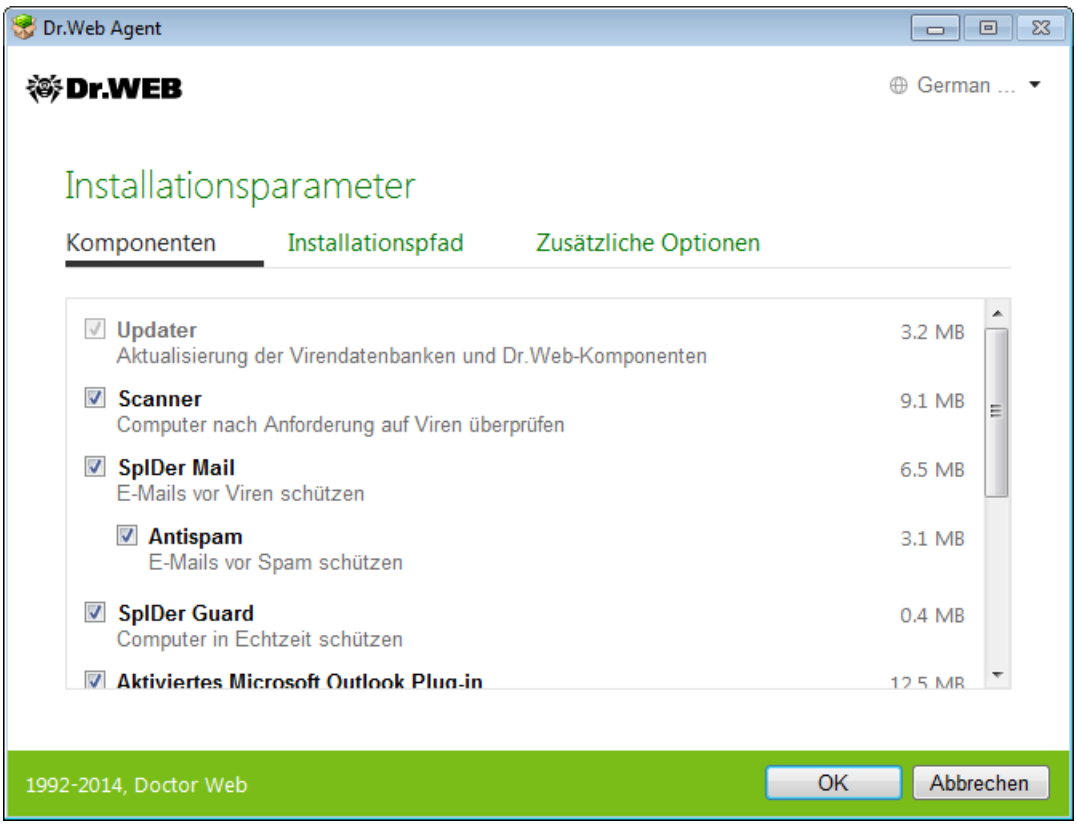
3. Wenn die Verbindung zum zentral verwalteten Virenschutz-Server erfolgreich hergestellt wurde, öffnet sich ein Dialogfenster mit der Meldung über die Bereitschaft zur Installation. Sie können den Installationsvorgang mit den Standardeinstellungen starten, indem Sie auf **Installieren** klicken.

Dr.Web Agent
Dr.WEB
German ...
Das System ist bereit für die Installation von Dr.Web Agent 10.0
Die Installation von Dr.Web Agent 10.0 auf einem Computer mit einem anderen installierten Antivirusprogramm bzw. einer Firewall kann unvorhersehbare Folgen nach sich ziehen (einschließlich des Ausfalls des Sicherheitssystems). Ist ein anderes Antivirusprogramm installiert, klicken Sie auf "Beenden", um die Installation abzubrechen, löschen Sie das andere Antivirusprogramm bzw. die Firewall und starten Sie den Installationsassistenten von Dr.Web Agent 10.0 neu.
Wenn Sie sich sicher sind, dass kein anderes Antivirusprogramm auf dem Computer installiert ist, klicken Sie auf Installieren.
Installationsparameter
1992-2014, Doctor Web
Zurück
Installieren
Beenden

Um die zu installierenden Komponenten selbständig auszuwählen, den Pfad der Installation sowie einige zusätzliche Parameter anzugeben, klicken Sie auf **Installationsparameter.** Diese Option ist für erfahrene Benutzer vorgesehen.

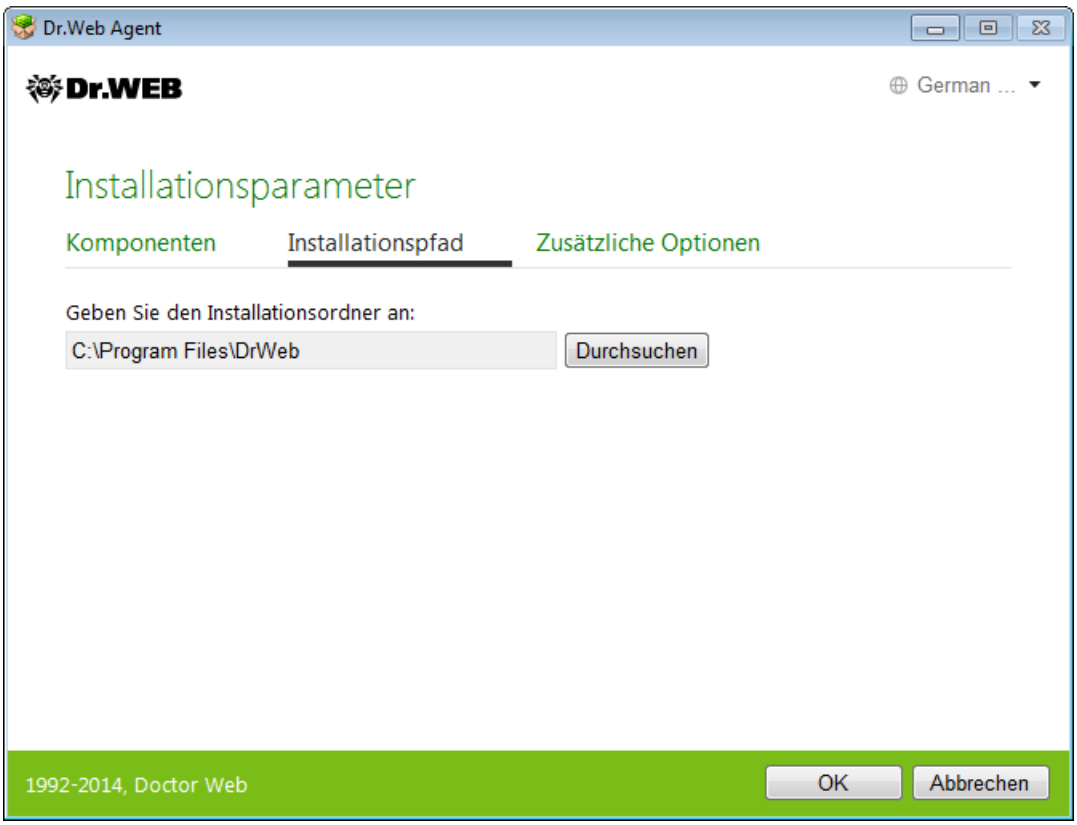
4. Haben Sie im vorherigen Abschnitt auf **Installieren** geklickt, gehen Sie zu der Beschreibung im Abschnitt 7 über. Andernfalls wird das Dialogfenster **Installationsparameter** geöffnet.

   Auf der Registerkarte **Komponenten** werden die für die Installation verfügbaren Komponenten von **Dr.Web** angezeigt.



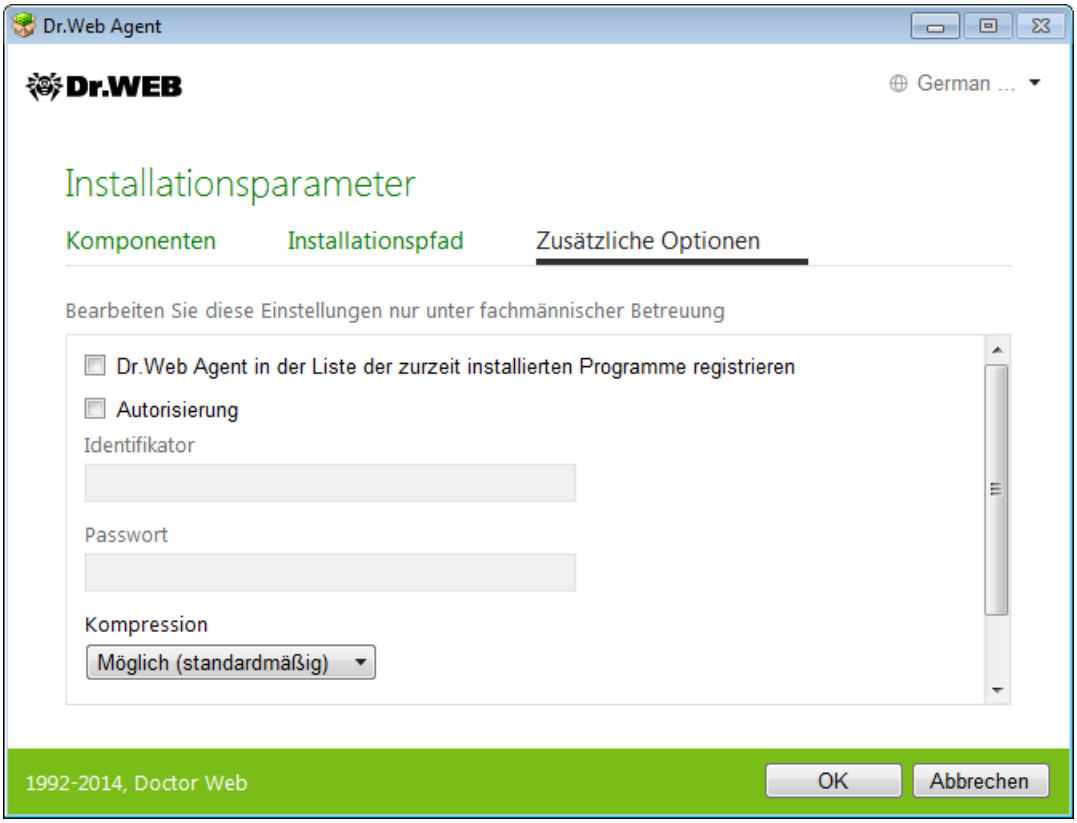
Markieren Sie die Kontrollkästchen neben den Komponenten, die Sie auf Ihrem Computer installieren wollen. Standardmäßig sind alle Komponenten mit Ausnahme von **Dr.Web Firewall** gewählt.

5. Auf der Registerkarte **Installationspfad** können Sie das Verzeichnis angeben, in dem **Dr.Web** installiert wird.



Standardmäßig wird das Programm ins DrWeb-Verzeichnis installiert, das sich im Verzeichnis Program Files auf der Systemplatte befindet. Um den Installationspfad zu ändern, klicken Sie auf **Durchsuchen** und geben Sie den gewünschten Pfad an.

6. Auf der nächsten Registerkarte wird Ihnen angeboten, zusätzliche Einstellungen vorzunehmen.



Gegebenenfalls können Sie das Kontrollkästchen **Dr.Web Agent in der Liste der zurzeit installierten Programme registrieren** aktivieren. Diese Option ermöglicht es unter anderem, **Dr.Web** mit Windows-Mitteln zu entfernen.

Zur manuellen Autorisierung auf dem zentral verwalteten Virenschutz-Server markieren Sie das entsprechende Kontrollkästchen. Danach legen Sie die Parameter zur Autorisierung der Station fest: deren **ID** auf dem Server sowie das **Passwort** für den Zugriff darauf. Dabei erhält die Station den Zugriff, ohne dass manuelle Bestätigung durch den Administrator auf dem Server benötigt wird.

Anhand von Dropdown-Listen **Komprimierung** und **Verschlüsselung** werden jeweils die Modi für den Datenverkehr zwischen dem Server und **Dr.Web** festgelegt.

Um vorgenommene Änderungen zu speichern, klicken Sie auf **OK.** Sie kehren dann zum vorherigen Dialog zurück.

Klicken Sie auf **Installieren.**

7. Es wird die Installation von **Dr.Web** gestartet. Es sind keine Eingriffe seitens des Benutzers notwendig.
8. Nach Installationsabschluss werden Sie vom Programm aufgefordert, den Computer neu zu starten. Klicken Sie auf **Jetzt neu starten.**

3.2. Installation mithilfe eines Installationspakets der Lite-Version

Um **Dr.Web** zu installieren, benötigen Sie die Administratorrechte.

Die Installation von **Dr.Web** kann in jedem der folgenden Modi durchgeführt werden:

- im Hintergrundmodus;
- im üblichen Modus.

Installation über Befehlszeile

Um die Installation von **Dr.Web** über die Befehlszeile zu starten, geben Sie in der Befehlszeile erforderliche Parameter an. Beim Starten des folgenden Befehls wird beispielsweise **Dr.Web** im Hintergrundmodus installiert:

```
drweb-ess-installer.exe /silent yes
```

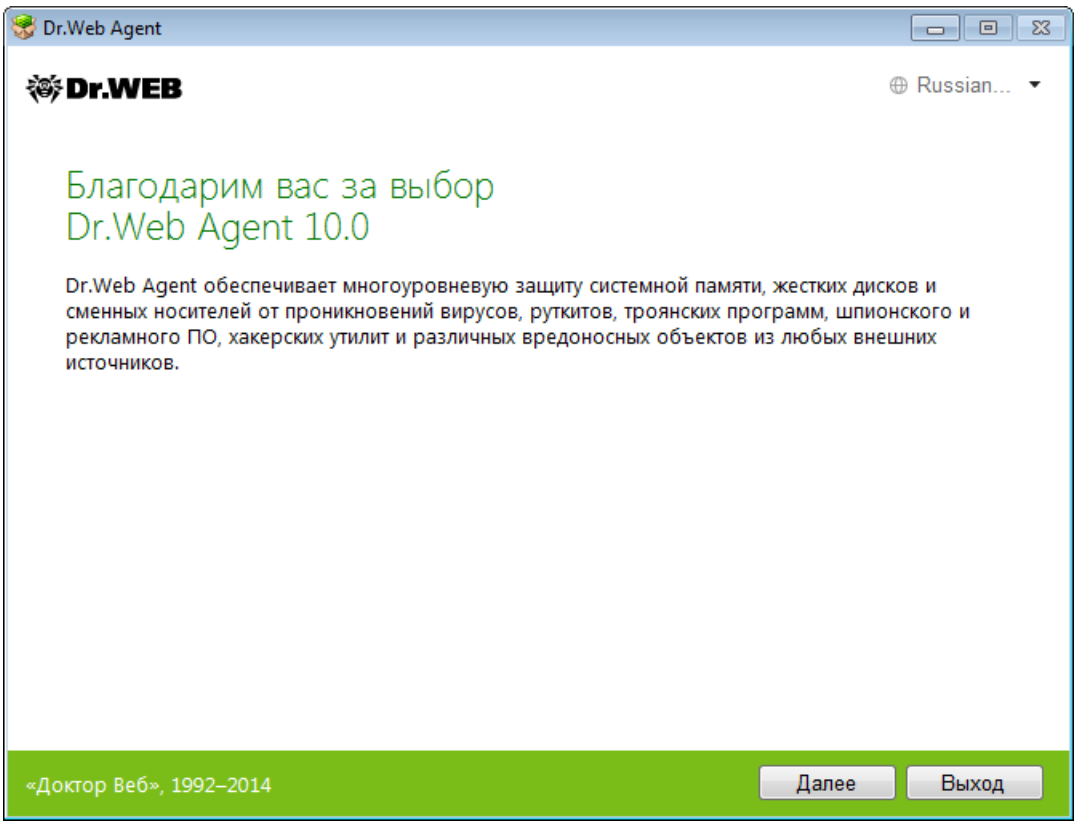
Alle verfügbaren Befehlszeilenparameter für Installationspakete finden Sie im Anhang A.

Installation im üblichen Modus

1. Starten Sie das Installationspaket, das Sie vom Administrator erhalten haben.

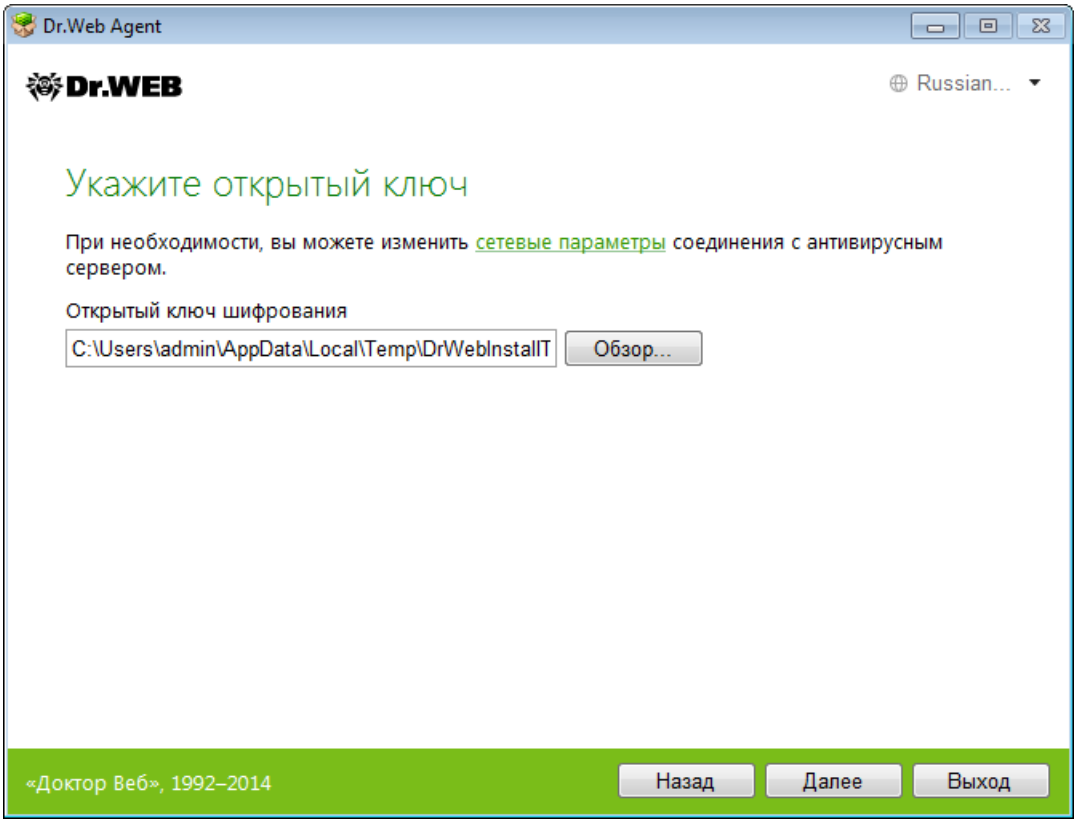
   Wurden andere Antivirusprogramme auf der Workstation bereits installiert, versucht der Installations-Assistent diese zu entfernen.Sollte die Deinstallation fehlgeschlagen sein, müssen Sie die auf der Workstation benutzte Antivirensoftware selbständig entfernen.

   Es öffnet sich das Dialogfeld des Installations-Assistenten von **Dr.Web**.



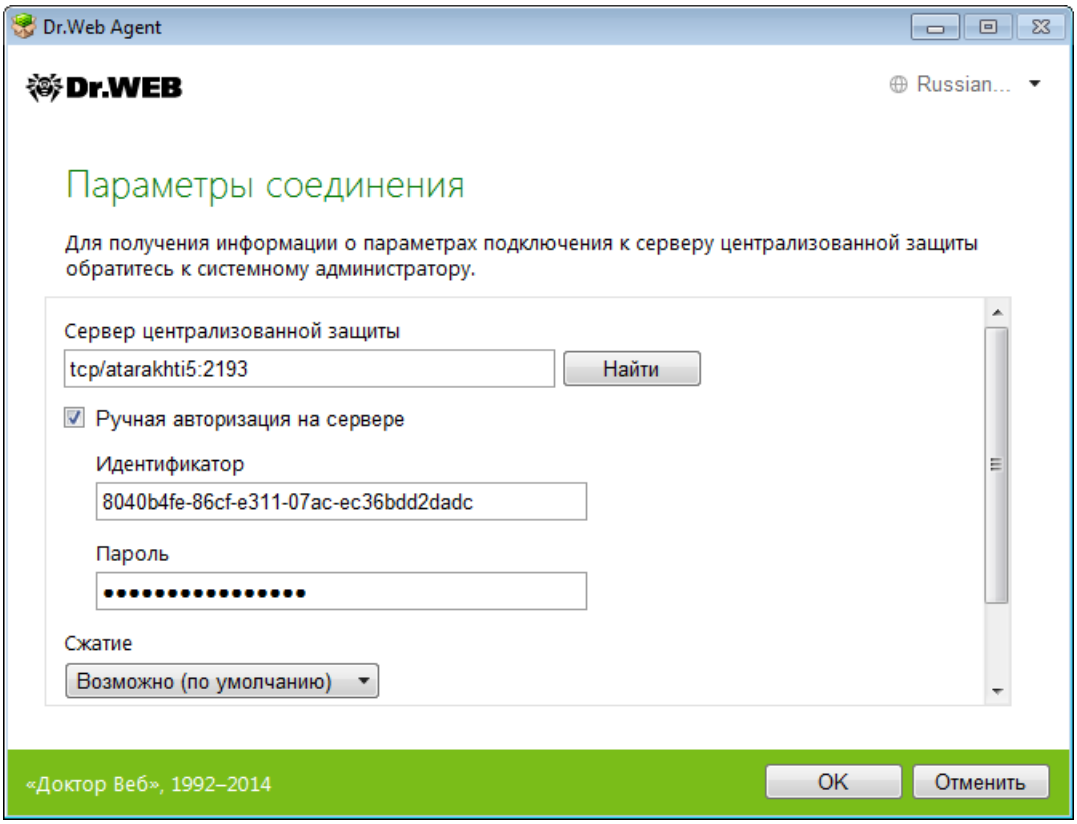
Klicken Sie auf **Weiter.**

2. Im nächsten Dialogfeld wird der vollständige Pfad des öffentlichen Verschlüsselungsschlüssels (drwcsd.pub) auf Ihrem Computer angegeben.



3. Sie können die Parameter der Netzwerkverbindung zum zentral verwalteten Virenschutz-Server ändern. Dazu klicken Sie auf entsprechenden Link im Dialogfeld. Es öffent sich dabei das Dialogfeld **Verbindungsparameter.**

Es wird ausdrücklich empfohlen, keine Änderungen ohne Zustimmung des Administrators Ihres Antivirus-Netzwerks vorzunehmen.



Für Informationen zu Verbindungsparameter zum zentral verwalteten Virenschutz-Server kontaktieren Sie bitte den Administrator.

Im Feld **Zentral verwalteter Virenschutz-Server** wird die Netzwerkadresse des Servers festgelegt, von dem **Dr.Web** installiert wird. Das feld wird automatisch ausgefüllt. Dabei werden die Daten des Servers angegeben, auf dem die Installationsdatei erstellt wurde.

Zur manuellen Autorisierung auf dem Server markieren Sie das entsprechende Kontrollkästchen. Danach legen Sie die Parameter zur Autorisierung der Station fest: deren **ID** auf dem Server sowie das **Passwort** für den Zugriff darauf. Dabei erhält die Station den Zugriff, ohne dass manuelle Bestätigung durch den Administrator auf dem Server benötigt wird.

Wird **Dr.Web** anhand der Installationsdatei installiert, die im **Dr.Web Verwaltungscenter** erstellt wurde, werden die Felder **ID** und **Passwort** bei manueller Autorisierung automatisch ausgefüllt.

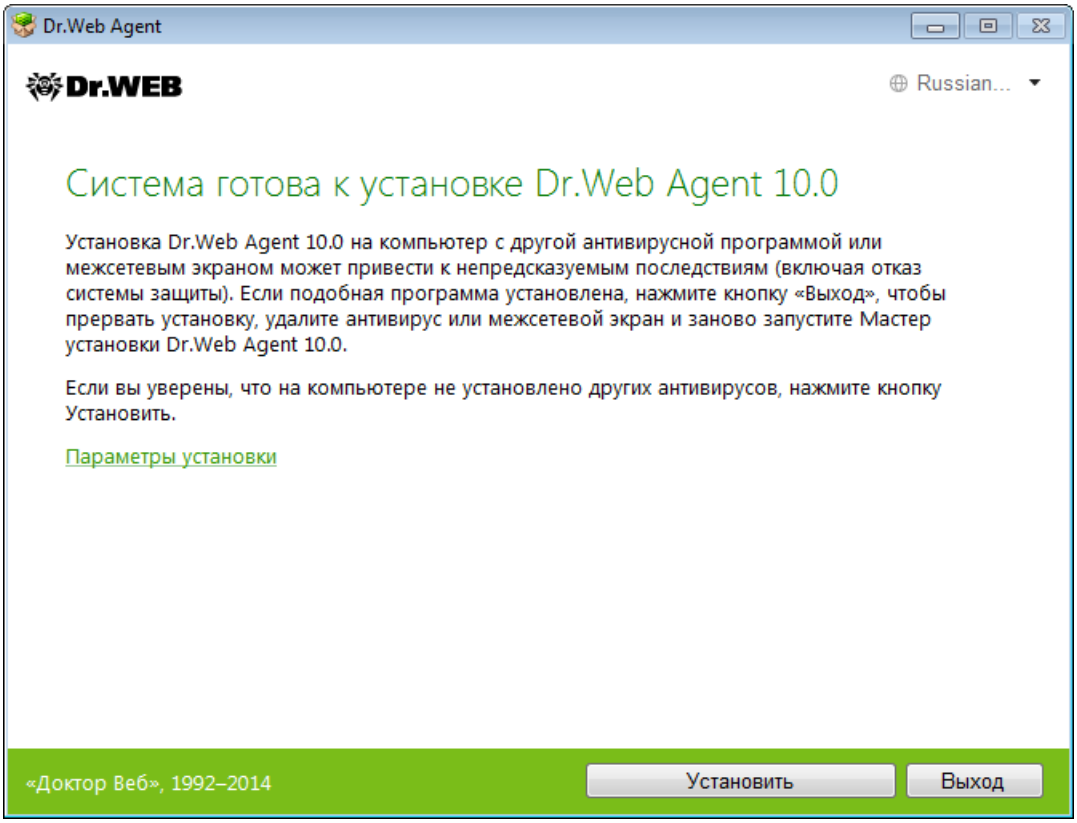
Anhand von Dropdown-Listen **Komprimierung** und **Verschlüsselung** werden jeweils die Modi für den Datenverkehr zwischen dem Server und **Dr.Web** festgelegt.

Um vorgenommene Änderungen zu speichern, klicken Sie auf **OK.** Sie kehren dann zum vorherigen Dialog zurück.

Klicken Sie auf **Weiter.** Es wird das Verfahren zur Herstellung der Verbindung zum Server gestartet.

Wenn keine Verbindung hergestellt wurde, folgen Sie dem Link und überprüfen Sie die Netzwerkparameter und/oder versuchen Sie den Verbindungsversuch erneut, indem Sie auf entsprechenden Button klicken.

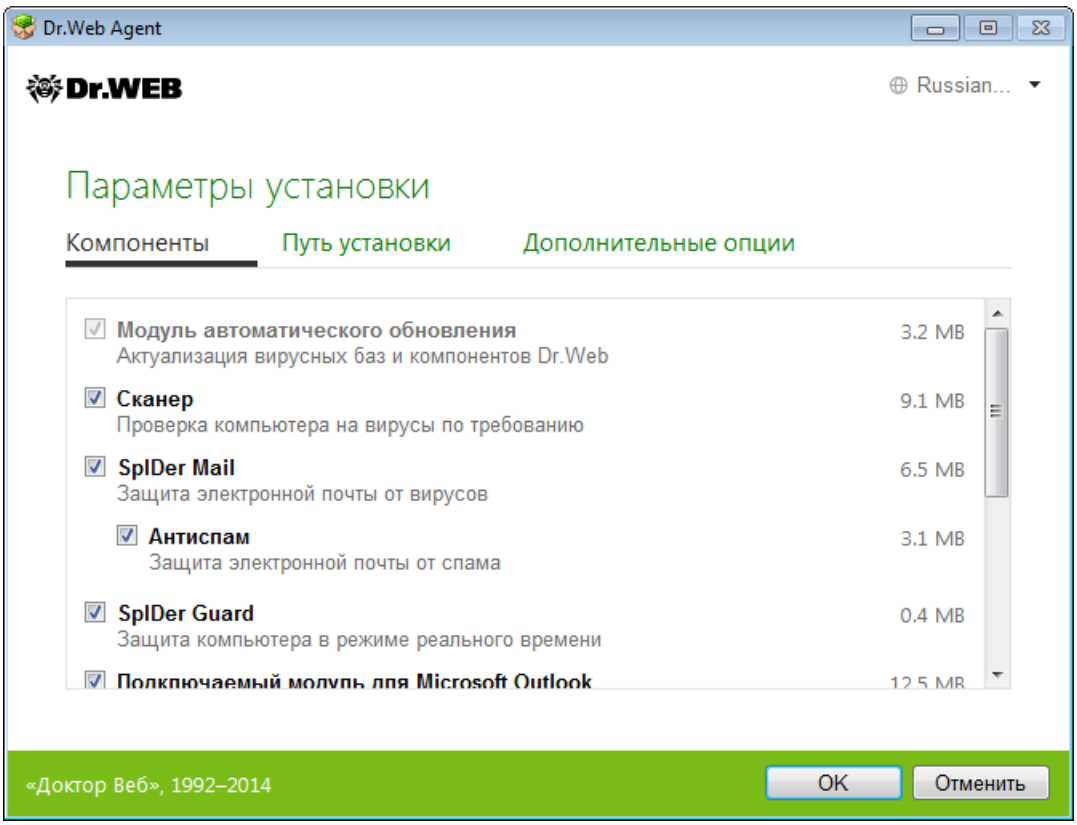
4. Wenn die Verbindung zum zentral verwalteten Virenschutz-Server erfolgreich hergestellt wurde, öffnet sich ein Dialogfenster mit der Meldung über die Bereitschaft zur Installation. Sie können den Installationsvorgang mit den Standardeinstellungen starten, indem Sie auf **Installieren** klicken.



Um die zu installierenden Komponenten selbständig auszuwählen, den Pfad der Installation sowie einige zusätzliche Parameter anzugeben, klicken Sie auf **Installationsparameter.** Diese Option ist für erfahrene Benutzer vorgesehen.

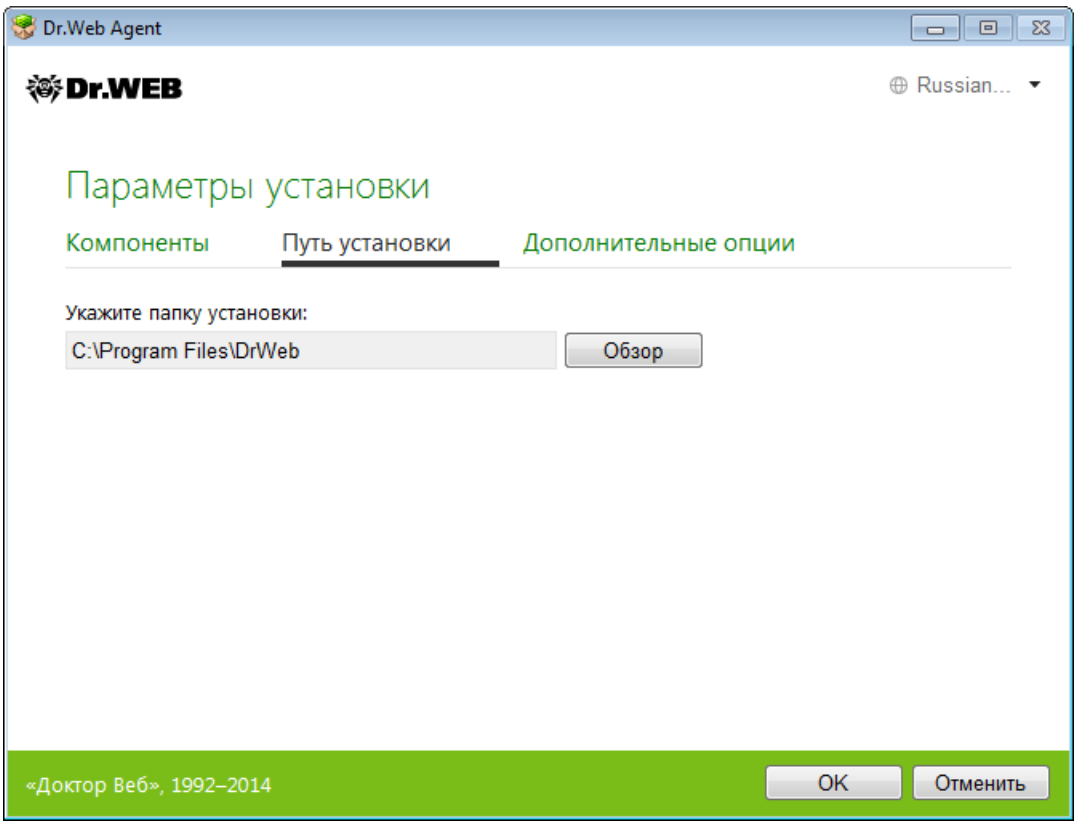
5. Haben Sie im vorherigen Abschnitt auf **Installieren** geklickt, gehen Sie zu der Beschreibung des Schritts 8. Anderenfalls wird das Dialogfenster **Installationsparameter** geöffnet.

   Auf der Registerkarte **Komponenten** werden die für die Installation verfügbaren Komponenten von **Dr.Web** angezeigt.



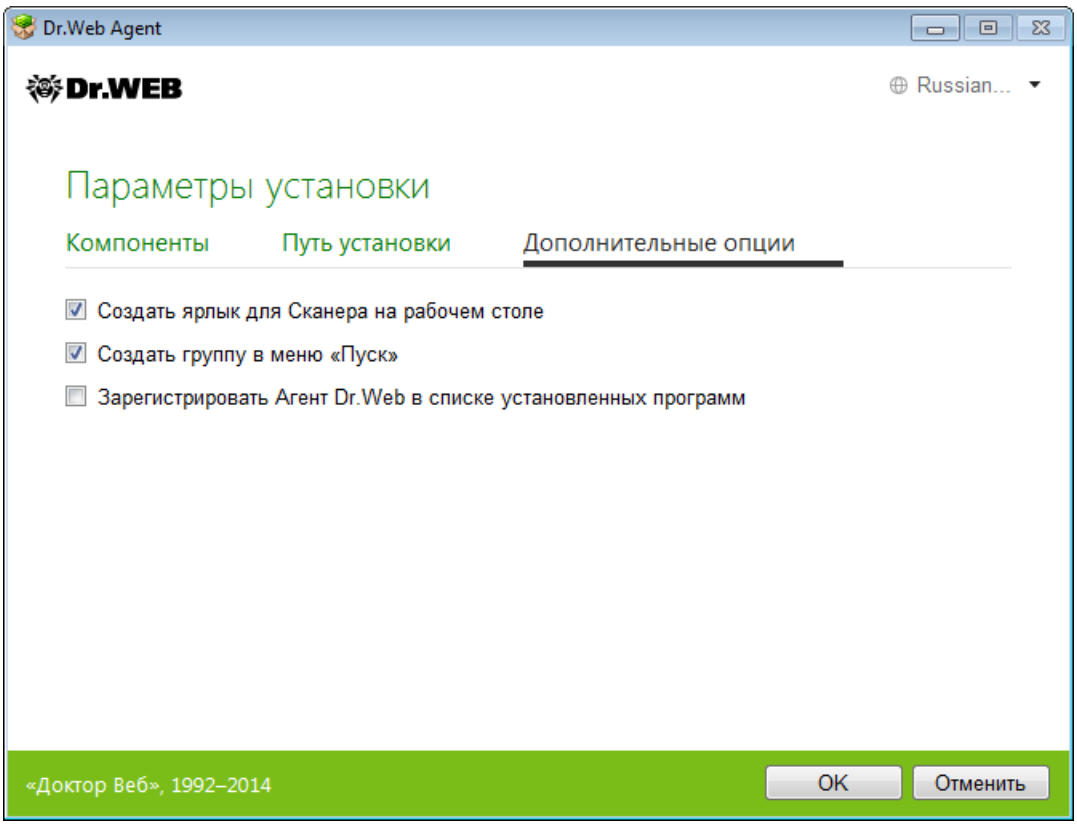
Markieren Sie die Kontrollkästchen neben den Komponenten, die Sie auf Ihrem Computer installieren wollen. Standardmäßig sind alle Komponenten mit Ausnahme von **Dr.Web Firewall** gewählt.

6. Auf der Registerkarte **Installationspfad** können Sie das Verzeichnis angeben, in dem **Dr.Web** installiert wird.



Standardmäßig wird das Programm ins DrWeb-Verzeichnis installiert, das sich im Verzeichnis Program Files auf der Systemplatte befindet. Um den Installationspfad zu ändern, klicken Sie auf **Durchsuchen** und geben Sie den gewünschten Pfad an.

7. Auf der Registerkarte **Zusätzliche Optionen** wird es Ihnen angeboten, die Erstellung von Verknüpfungen für den Start von **Dr.Web** einzustellen.



Gegebenenfalls können Sie das Kontrollkästchen **Dr.Web Agent in der Liste der zurzeit installierten Programme registrieren** aktivieren. Diese Option ermöglicht es unter anderem, **Dr.Web** mit Windows-Mitteln zu entfernen.

Um vorgenommene Änderungen zu speichern, klicken Sie auf **OK.** Sie kehren dann zum vorherigen Dialog zurück.

Klicken Sie auf **Installieren.**

8. Es wird die Installation von **Dr.Web** gestartet. Es sind keine Eingriffe seitens des Benutzers notwendig.
9. Nach Installationsabschluss werden Sie vom Programm aufgefordert, den Computer neu zu starten. Klicken Sie auf **Jetzt neu starten.**

3.3. Programm ändern bzw. deinstallieren

Um **Dr.Web** lokal entfernen zu können, muss diese Option durch den Administrator auf dem zentral verwalteten Virenschutz-Server erlaubt werden.

Nach der Deinstallation von **Dr.Web** wird Ihr Computer nicht mehr vor Viren und anderen schädlichen Programmen geschützt.

Dr.Web mit Windows-Bordmitteln entfernen oder ändern

Mit diesem Verfahren kann das Programm nur deinstalliert werden, wenn das Kontrollkästchen **Dr.Web Agent in der Liste der zurzeit installierten Programme registrieren** mit Hilfe des Installations-Assistenten markiert wurde.

Wenn **Dr.Web** im Hintergrundmodus installiert wurde, kann **Dr.Web** mit herkömmlichen Mitteln deinstalliert werden, wenn der Schlüssel `-regagent` bei der Installation verwendet wurde.

1. Um **Dr.Web** durch das Hinzufügen und Entfernen einzelner Komponenten zu deinstallieren oder die Konfiguration davon zu ändern, starten Sie das Windows-Tool zum Entfernen von Programmen.
2. In der geöffneten Liste wählen Sie die Zeile mit dem Programmnamen. Um das Programm vollständig zu entfernen klicken Sie auf **Entfernen** und gehen Sie zum Schritt 6. Klicken Sie zur Änderung der Konfiguration von **Dr.Web** durch das Hinzufügen und Entfernen einzelner Komponenten auf **Ändern**. Es öffnet sich dabei das Dialogfenster des Tools zum Entfernen und Ändern der Komponenten des Programms.
3. Wenn es erforderlich ist, den Virenschutz auf Ihrem Computer wiederherzustellen, wählen Sie im geöffneten Fenster den Punkt **Programm wiederherstellen**.
4. Zum Ändern der Konfiguration von **Dr.Web** wählen Sie den Punkt **Komponenten ändern.** Im geöffneten Fenster markieren Sie die Kontrollkästchen neben den Komponenten, die Sie hinzufügen wollen, und entfernen Sie die Markierung neben den Komponenten, die zu löschen sind. Nachdem Sie Ihre Wahl getroffen haben, klicken Sie auf **Installieren**.
5. Um alle installierten Komponenten zu entfernen, wählen Sie den Punkt **Programm löschen**.
6. Aktivieren Sie im Fenster **Parameter** die Kontrollkästchen neben den Daten, die Sie nach der Deinstallation des Programms beibehalten wollen. Die beibehaltenen Objekte und Einstellungen können vom Programm bei wiederholter Installation verwendet werden. Standardmäßig sind alle Optionen aktiviert: **Quarantäne**, **Einstellungen von Dr.Web Agent** und **Geschützte Dateikopien**. Klicken Sie auf **Weiter**.
7. Um das Entfernen von **Dr.Web** zu bestätigen, klicken Sie auf **Löschen**.
8. Sie werden vom Programm aufgefordert, den Computer neu zu starten, um das Verfahren zum Entfernen bzw. Ändern der Komponenten von **Dr.Web** abzuschließen.

Über die Befehlszeile entfernen

Um **Dr.Web** über die Befehlszeile zu entfernen, geben Sie in der Befehlszeile den Namen der ausführbaren Datei (win-es-agent-setup.exe) und die gewünschten Optionen ein.

Die Datei win-es-agent-setup.exe befindet sich im Verzeichnis C:\ProgramData\Doctor Web\Setup\.

Bei dem folgenden Beispielbefehl wird **Dr.Web** im Hintergrundmodus entfernt und anschließend erfolgt ein automatischer Neustart des Systems:

```
win-es-agent-setup.exe /instMode remove /silent yes
```

4. Erste Schritte

Nach der Installation von **Dr.Web** erscheint im Windows-Infobereich das Symbol des **SpIDer Agenten** .

Das Symbol des **SpIDer Agenten** wird im Infobereich nicht angezeigt, wenn der Administrator Ihres Antivirus-Netzwerks die entsprechende Option auf dem zentral verwalteten Virenschutz-Server aktiviert hat.

Falls **SpIDer Agent** nicht gestartet wurde, klicken Sie auf **Start,** öffnen Sie den Ordner **Dr.Web** und wählen Sie **SpIDer Agent.**

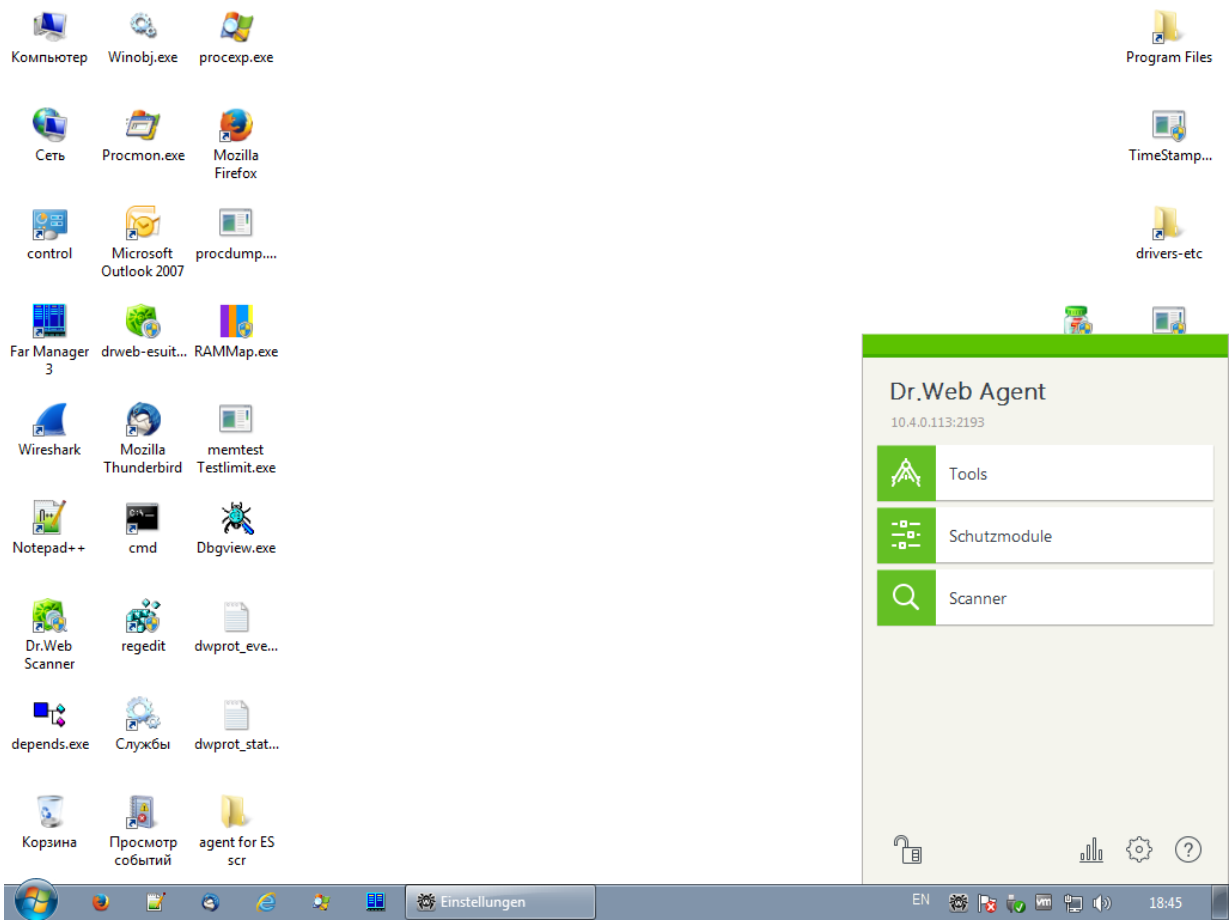
Das Symbol des **SpIDer Agenten** zeigt den aktuellen Status von **Dr.Web** an:

- – alle Komponenten, die für den Systemschutz dienen, sind gestartet und laufen korrekt, die Verbindung zum zentral verwalteten Virenschutz-Server ist hergestellt;
- – **Dr.Web** Selbstschutz oder eine wichtige Komponente (**SpIDer Guard**, **Firewall**) ist deaktiviert. Dies verringert das Sicherheitsniveau des Antivirenprogramms oder des Rechners. Ein anderer Grund ist, dass auf die Verbindungen mit dem Server wird gewartet. Der Server hat möglicherweise die Verbindung mit der Workstation zurückgewiesen bzw. den Zugriff auf seine Ressourcen verweigert. Aktivieren Sie den Selbstschutz oder die deaktivierte Komponente, warten Sie, bis die Verbindungen mit dem Server hergestellt wird, oder wenden Sie sich an den Administrator Ihres Antivirus-Netzwerks, falls die Verbindung nicht hergestellt werden kann;
- – Komponenten werden erst nach dem Start des Betriebssystems gestartet, warten Sie deswegen den Start der Komponenten des Programms ab; oder beim Starten einer der wichtigen **Dr.Web** Komponenten ist ein Fehler aufgetreten, der Rechner kann infiziert werden. Falls sich das Symbol nicht ändert, wenden Sie sich an den Administrator Ihres Antivirus-Netzwerks.

Weiterhin können, je nach Einstellungen, diverse Info-Meldungen oberhalb vom Symbol des **SpIDer Agenten** angezeigt werden.

Um das Menü von **SpIDer Agent** aufzurufen, klicken Sie im Windows-Infobereich auf das Symbol von **SpIDer Agent** .

Um Einstellungen vornehmen oder Schutzmodule verwalten bzw. deaktivieren zu können, müssen Sie Administratorrechte besitzen.



Im Menü von **SpIDer Agent** befinden sich die wichtigsten Verwaltungstools von **Dr.Web**.

Tools. Öffnet das Menü, über das Sie zu den folgenden Bereichen wechseln können:

- Quarantänemanager;
- Support.

Schutzmodule. Ermöglicht einen Schnellzugriff auf die Liste der Schutzmodule, in der Sie jeden der Schutzmodule aktivieren bzw. deaktivieren können.

Scanner. Ermöglicht den Schnellzugriff auf die Scannmodi.

Betriebsmodus. Ermöglicht eine schnelle Umschaltung zwischen Benutzer und Administrator. Standardmäßig wird **Dr.Web** im eingeschränkten Modus gestartet. In diesem Modus kann der Benutzer auf die Einstellungen und die Einstellungen der Schutzmodule nicht zugreifen. Um in den anderen Modus zu wechseln, klicken Sie auf das Schlosssymbol. Wenn die Benutzerkontensteuerung aktiviert ist, werden erweiterte Rechte angefordert. Außerdem müssen Sie dabei ein Passwort eingeben, wenn im Bereich Einstellungen die Option **Dr.Web Einstellungen mit Passwort schützen** aktiviert ist.

Statistiken. Öffnet das Fester, das statistische Daten für die laufende Sitzung jedes Schutzmoduls (z.B. Informationen zur Anzahl von gescannten, infizierten und verdächtigen Objekten, vorgenommen Aktionen usw.) enthält.

Einstellungen. Öffnet das Fenster mit den allgemeinen Einstellungen, Einstellungen der Schutzmodule und von **Office Control** sowie Ausnahmenlisten.

Es ist nicht möglich, die Einstellungen zu ändern bzw. eine Komponente zu deaktivieren, wenn der Administrator des Zentralschutz-Servers, mit dem **Dr.Web** verbunden wird, diese Aktionen nicht erlaubt hat.

Um auf die Einstellungen der Komponenten zuzugreifen, wird auch ein Passwort benötigt, wenn Sie im Abschnitt Einstellungen das Kontrollkästchen **Dr.Web Einstellungen mit Passwort schützen** aktiviert haben.

Sollten Sie das Passwort für Produkteinstellungen vergessen haben, kontaktieren Sie den Administrator Ihres Antivirus-Netzwerks.

4.1. Antivirus überprüfen

Testen Sie Ihre Antivirusprogramme, die Viren durch ihre Signatur mit Hilfe einer EICAR (European Institute for Computer Anti-Virus Research) Test-Datei erkennen.

Viele Entwickler von Antivirensoftware haben dafür das Standardprogramm test.com hervorgebracht. Dieses Programm wurde speziell entwickelt, um dem Benutzer zu zeigen, wie das installierte Antivirusprogramm ihn bei Virenfund warnt. Der Rechner des Benutzers wird dabei nicht gefährdet. Das Programm Test.com ist nicht böswillig, wird aber von den meisten Antivirenprogrammen als Virus eingestuft. **Dr.Web Agent** nennt diesen „Virus" wie folgt: `EICAR Test File (Not a Virus!)`. Ähnlich wird es von anderen Antivirusprogrammen genannt.

Das Programm test.com ist eine 68-Byte-COM-Datei. Beim Ausführen der Datei wird eine Meldung angezeigt: `EICAR-STANDARD-ANTIVIRUS-TEST-FILE!`

Die Datei test.com besteht ausschließlich aus Zeichen, die folgende Zeile bilden:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H
+H*
```

Wenn Sie die Datei test.com, die oben genannte Zeile beinhaltet, generieren, wird es als oben beschriebenes „Virus" gemeldet.

Im optimalen Modus wird der Start der EICAR-Testdatei von **SpIDer Guard** nicht unterbrochen und diese Operation nicht als gefährlich definiert, da diese Datei keine Gefahr für den Computer darstellt. Wird allerdings solche Datei auf dem Computer kopiert bzw. erstellt, bearbeitet **SpIDer Guard** die Datei als ein gefährliches Programm und verschiebt sie standardmäßig in die **Quarantäne**.

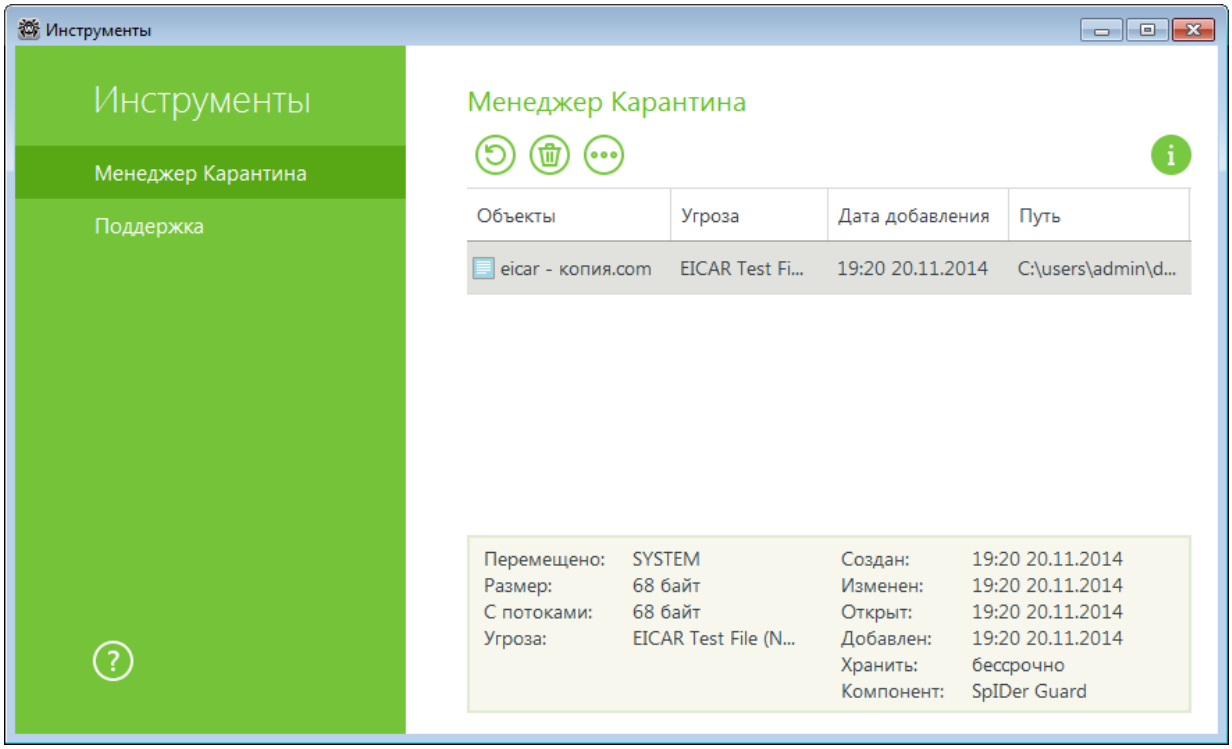
5. Tools

5.1. Quarantänemanager

Quarantänemanager enthält die Informationen über den Inhalt der Quarantäne, die zur Isolation von verdächtigen Dateien dient. Außerdem werden Backup-Kopien von Dateien in die Quarantäne verschoben, die von **Dr.Web** behandelt wurden.

In den Einstellungen vom Quarantänemanager können Sie auch die Option aktivieren, die den Modus für die Isolierung der infizierten Objekte bestimmt, die auf den Wechseldatenträgern entdeckt wurden. Bei der aktivierten Option werden die Bedrohungen dieser Art in einem Verzeichnis auf dem gleichen Datenträger gespeichert und nicht verschlüsselt. Dabei wird ein Quarantäne-Verzeichnis nur dann erstellt, wenn die Speicherung auf dem Datenträger möglich ist. Die Verwendung gesonderter Verzeichnisse und Verzicht auf die Verschlüsselung erlauben es, dem möglichen Datenverlust vorzubeugen.

Um zu diesem Fenster zu wechseln, wählen Sie im Untermenü **Tools** des Menüs **SpIDer Agent** den Punkt **Quarantänemanager**.



Im mittleren Bereich des Fensters wird eine Info-Tabelle über den Status der Quarantäne angezeigt, die folgende Felder enthält:

- **Objekte –** Liste mit den Namen der Objekte, die sich zurzeit in der Quarantäne befinden;
- **Bedrohung** – Typ eines bösartigen Programms, der von **Dr.Web** beim automatischen Verschieben des Objektes in die Quarantäne bestimmt wird;
- **Hinzugefügt am** – Datum der Verschiebung der Datei in die Quarantäne;
- **Pfad** – der vollständige Pfad zum Ort, in dem sich das Objekt vor dem Verschieben in die Quarantäne befand.

Die Dateien im **Quarantänemanager** sind nur für dazu berechtigte Benutzer sichtbar. Um ausgeblendete Objekte anzeigen zu lassen, sind die Administratorrechte erforderlich.

Im Kontextmenü sind die folgenden Optionen verfügbar:

- **Wiederherstellen** – Datei unter dem angegebenen Namen in den gewünschten Ordner verschieben;

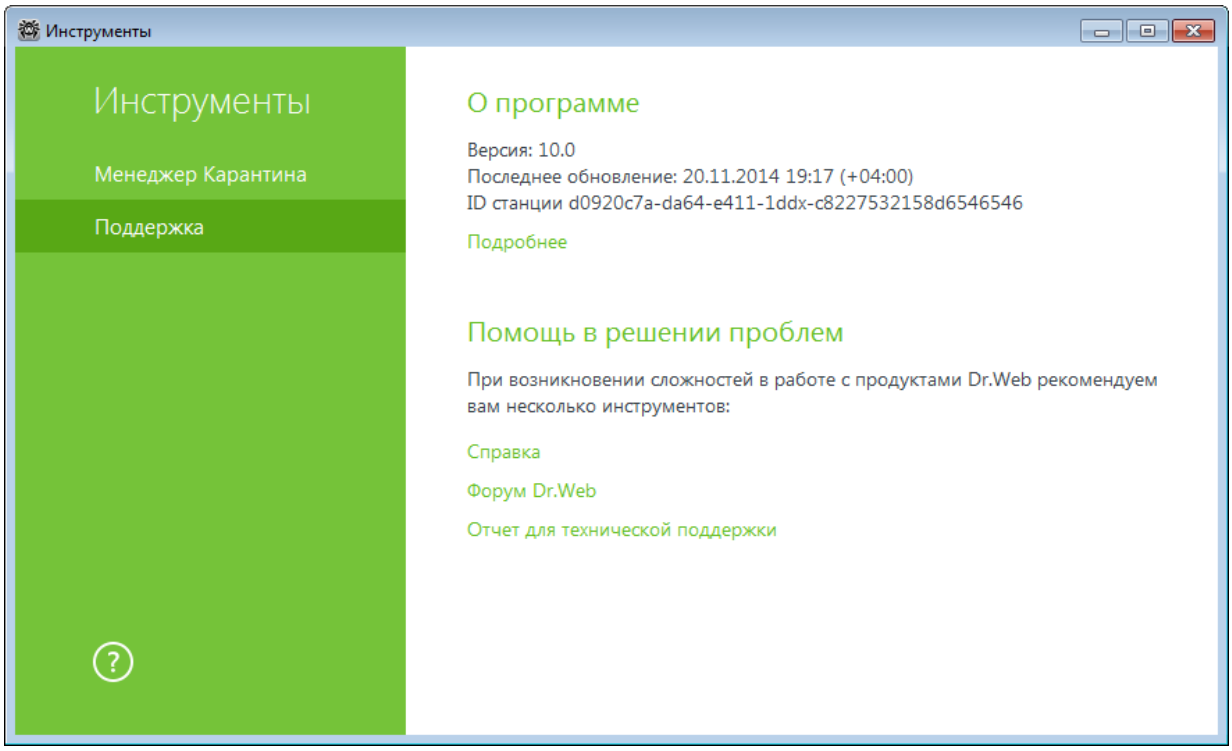
  Nutzen Sie diese Funktion nur im Fall, wenn Sie sichergestellt haben, dass das Objekt zuverlässig ist.

- **Entfernen –** Datei sowohl aus der Quarantäne als auch aus dem System entfernen.

Um alle Objekte in der Quarantäne zu löschen, klicken Sie auf und wählen Sie in der Dropdown-Liste **Alle löschen**.

5.2. Support

Dieser Bereich enthält Information zur Produktversion, zu den Schutzmodulen und Komponenten, dem Datum der letzten Aktualisierung sowie nützliche Links, auf denen Sie eventuelle Antworten auf Ihre Fragen oder Hilfe für die Behebung von Problemen mit **Dr.Web** erhalten können.



Wenn Sie Fragen haben, wählen Sie eine der folgenden Optionen aus.

Hilfe. Öffnet das Hilfefenster.

Dr.Web Foren. Öffnet das **Dr.Web** Forum unter http://forum.drweb.com.

Bericht für technischen Support. Öffnet den Assistenten zum Erstellen von Berichten, die wichtige Informationen über den Status und Zustand des Betriebssystems enthalten.

Wenn Sie es nicht geschafft haben, das Problem zu lösen, dann können Sie die Webform im entsprechenden Abschnitt unter http://support.drweb-av.de ausfüllen.

Die Vertretung von **Doctor Web** in Ihrer Nähe und alle notwendigen Informationen für Benutzer können Sie unter http://company.drweb-av.de/ finden.

5.2.1. Bericht erstellen

Bei Anfrage an den Administrator Ihres Antivirus-Netzwerks können Sie einen Bericht über Ihr Betriebssystem und Betrieb von **Dr.Web** erstellen.

Der Bericht wird in Archivform im Doctor Web Verzeichnis, das sich im Benutzerprofil-Ordner %USERPROFILE% befindet, gespeichert.

Um einen Bericht zu erstellen, klicken Sie die entsprechende Schaltfläche an. Der Bericht kann diefolgenden Angaben enthalten:

1. Technische Daten zu Betriebssystem:
   - Gesamtangaben zu PC;
   - gestartete Vorgänge;
   - geplante Aufgaben;
   - Dienste, Treiber;
   - Default-Browser;
   - installierte Anwendungen;
   - Richtlinien für Softwareeinschränkungen;
   - HOSTS-Datei;
   - DNS-Server;
   - Einträge im Ereignisprotokoll;
   - Liste der Systemordner;
   - Schlüssel der Registrierdatenbank;
   - Winsock-Dienstanbieter;
   - Netzwerkverbindungen;
   - Protokolle vom Dr.Watson Debugger;
   - Leistungsindex.
2. Informationen zu folgenden Produkten von **Dr.Web**.
3. Informationen zu Modulen von **Dr.Web**:
   - **Dr.Web für IBM Lotus Domino**;
   - **Dr.Web für Kerio MailServer**;
   - **Dr.Web für Kerio WinRoute**.

Informationen über den Betrieb von **Dr.Web Antivirus-Lösungen** finden Sie im Windows-Ereignisprotokoll, Abschnitt **Anwendungs- und Dienstprotokolle** → **Doctor Web.**

6. Dr.Web Scanner

Dr.Web Scanner für Windows scannt Bootsektoren, Speicher, einzelne Dateien und Objekte sowie Objekte mit komplexer Datenstruktur (Archive, Container, E-Mails mit Anhängen). Bei der Suche werden alle Techniken zum Erkennen von Bedrohungen eingesetzt. Der **Dr.Web Scanner** verwendet standardmäßig sowohl signaturbasierte Ansätze als auch heuristischen Suchverfahren (diese Technik versucht, sowohl neue als auch bekannte Formen von Viren effizienter zu erkennen, indem sie nach allgemeinen Vireneigenschaften sucht). Komprimierte ausführbare Dateien werden beim Scanvorgang entpackt. Dabei können Objekte in Archiven aller wichtigen Formate (ACE, ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP usw.), in Containerdateien (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM usw.) sowie in E-Mails (das Format der E-Mails muss dem Standard RFC822 entsprechen), die sich in Postfächern Ihrer E-Mail-Programme befinden, überprüft werden.

Bei der Entdeckung eines Schadobjektes werden Sie vom **Dr.Web Scanner** nur über die Gefahr gewarnt. Der Bericht mit Scanergebnissen wird in einer Tabelle angezeigt. Dort können Sie notwendige Aktion zur Behandlung des entdeckten schädlichen oder verdächtigen Objektes auswählen. Sie können sowohl die Standard-Aktion auf alle entdeckten Bedrohungen anwenden als auch ein bestimmtes Verfahren zur Behandlung einzelner Objekte wählen.

Die Standard-Aktionen sind optimal für die meisten Anwendungen. Bei Bedarf können Sie diese allerdings in dem Einstellungsfenster für Parameter des **Dr.Web Scanners** ändern. Eine Aktion für ein einzelnes Objekt können Sie am Ende der Überprüfung wählen. Die allgemeinen Einstellungen für die Neutralisierung bestimmter Bedrohungstypen müssen aber vor Beginn der Überprüfung definiert werden.

6.1. Suchlauf starten

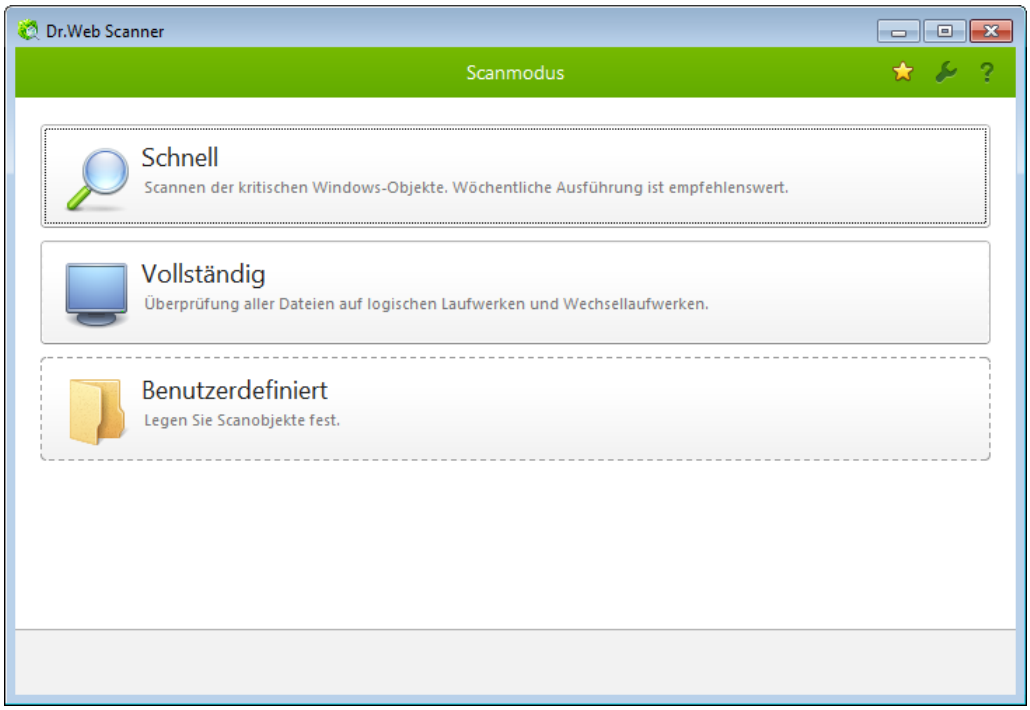
Scanner starten

Es empfiehlt sich, den **Scanner** als Benutzer mit administrativen Rechten zu starten. Anderenfalls werden Dateien und Ordner (darunter Systemordner), auf die der Benutzer keinen Zugriff hat, nicht gescannt.

1. Sie startet den **Scanner** über einen der folgenden Wege:
   - durch Anklicken des Symbols vom **Scanner** auf dem Desktop;
   - durch Aufruf des Punkts **Scanner** im Menü **SpIDer Agent** im Windows-Infobereich;
   - durch den Menüpunkt **Dr.Web Scanner** im Ordner **Dr.Web** des Windows-Startmenüs (aufrufbar über **Start**);
   - über den entsprechenden Befehl in der Windows-Befehlszeile (mehr dazu finden Sie unter Scanner über die Befehlszeile starten).

   Um eine Datei oder einen Ordner mittels des **Scanners** mit Standardeinstellungen zu scannen, wählen Sie im Kontextmenü der Datei oder des Ordners (auf dem Desktop oder im Windows-Explorer) den Punkt **Mit Dr.Web prüfen**.

2. Nach dem Start des **Scanners** öffnet sich sein Hauptfenster.



Wenn Sie den **Scanner** zur Prüfung einer Datei oder eines Ordners starten, wird das ausgewählte Objekt sofort gescannt.

3. Zur Verfügung stehen drei Scanmodi: **Schnell**, **Vollständig** und **Benutzerdefiniert**.

   Beim *schnellen Scan* werden die folgenden Objekte gescannt:

   - Bootsektoren auf allen Laufwerken;
   - Arbeitsspeicher;
   - Root-Ordner des Boot-Laufwerkes;
   - Windows-Systemordner;
   - Ordner Eigene Dateien;
   - Temporäre Dateien;
   - Systemwiederherstellungspunkte;
   - Vorhandensein der Rootkits (wenn die Überprüfung im Administratormodus durchgeführt wird).

   Beim schnellen Scan werden keine Archive und E-Mail-Dateien geprüft.

   Beim *vollständigen Scan* werden der Hauptspeicher und alle Festplatten (einschließlich Bootsektoren) vollständig gescannt. Es wird auch nach Rootkits gesucht.

   Beim *benutzerdefinierten Scan* kann der Benutzer selbst die zu scannenden Dateien und Ordner auszuwählen.

4. Beim benutzerdefinierten Scan können im Fenster des **Scanners** die zu scannenden Objekte ausgewählt werden: beliebige Dateien und Ordner sowie Objekte wie Arbeitsspeicher, Boot-Sektoren usw.Um die ausgewählten Objekte zu scannen, klicken Sie auf **Prüfung starten**. Bei der schnellen bzw. vollständigen Prüfung ist die Auswahl der Objekte nicht erforderlich.
5. Nachdem das Scannen gestartet wird, werden die **Pause-** und **Stop-**Buttons im rechten

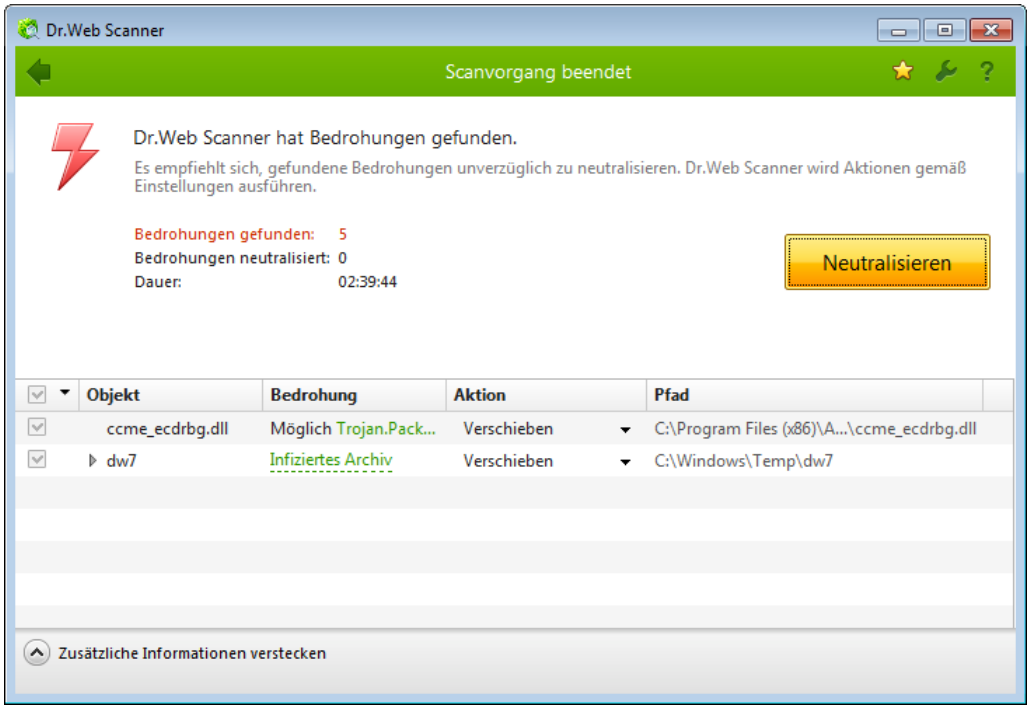
Fensterbereich verfügbar sein. Auf jeder Prüfungsstufe können Sie wie folgt vorgehen:

- klicken Sie auf **Pause**, um die Prüfung anzuhalten. Um die Prüfung fortzusetzen, klicken Sie auf **Fortfahren;**
- um die Prüfung abzubrechen, klicken Sie auf **Stop**.

Die Schaltfläche **Pause** ist während der Überprüfung des Arbeitsspeichers und der Prozesse nicht aktiv.

6.2. Aktionen bei Bedrohungserkennung

Nach Abschluss der Überprüfung informiert der **Dr.Web Scanner** lediglich über die entdeckten Bedrohungen und bietet die optimalsten Aktionen zur Neutralisierung an. Sie können alle entdeckten Bedrohungen gleichzeitig neutralisieren. Klicken Sie dazu nach Abschluss der Überprüfung auf **Neutralisieren** und **Dr.Web Scanner** wird die optimalen standardmäßigen Aktionen für alle entdeckten Bedrohungen ausführen.



Beim Klicken auf **Neutralisieren** werden Aktionen für die in der Tabelle ausgewählten Objekte ausgeführt. Standardmäßig sind alle Objekte nach Abschluss der Überprüfung für die Neutralisierung ausgewählt. Bei Bedarf können Sie bestimmte Objekte bzw. Gruppen von Objekten, für welche die Aktion **Neutralisieren** ausgeführt werden soll, manuell auswählen. Benutzen Sie dazu die Kontrollkästchen neben den Objektnamen bzw. das Dropdown-Menü in der Tabellenüberschrift.

Auswahl der Aktion

1. Wählen Sie die nötige Aktion für jedes Objekt im Feld **Aktion** in der Dropdown-Liste aus (standardmäßig wird der optimale Wert vom **Dr.Web Scanner** vorgeschlagen).
2. Klicken Sie auf **Neutralisieren.** **Dr.Web Scanner** wird alle erkannten Bedrohungen gleichzeitig neutralisieren.

Es bestehen folgende Einschränkungen:

- Desinfizieren verdächtiger Objekte ist unmöglich;
- Verschieben oder Löschen der Objekte, die keine Dateien sind (z.B. Bootsektoren), ist unmöglich;
- Beliebige Aktionen für einzelne Dateien innerhalb Archive, Installationspakete oder E-Mails sind unmöglich: Die Aktion wird in diesem Fall für das ganze Objekt ausgeführt.

Der ausführliche Bericht über den Betrieb des Programms wird in Form der Protokolldatei dwscanner.log im Ordner %USERPROFILE%\Doctor Web abgespeichert.

Spaltenname	Beschreibung

Objekt	In dieser Spalte wird der Name des infizierten bzw. verdächtigen Objektes (Dateiname – wenn es um eine infizierte Datei, **Boot sector,** wenn es um einen infizierten Bootsektor, **Master Boot Record,** wenn es um ein infiziertes Festplatten-MBR geht) angegeben.
Bedrohung	In dieser Spalte wird der Virusname bzw. der Name der Virusmodifikation nach interner Klassifikation von **Doctor Web** angegeben (als Modifikation eines bekannten Virus wird der Viruscode bezeichnet, der durch eine Änderung des bekannten Virus erstellt wird, sodass er vom Scanner zwar erkannt wird, aber die Algorithmen der Desinfizierung für den Ausgangsvirus dafür nicht verwendet werden können). Für verdächtige Objekte wird angegeben, dass „Objekt möglicherweise infiziert" ist und es wird der mögliche Virustyp nach der Klassifizierung der heuristischen Analyse angezeigt.
Aktion	Klicken Sie auf den Pfeil auf dieser Schaltfläche, um die Aktion für die gewählte Bedrohung zu definieren (standardmäßig bietet **Dr.Web Scanner** den optimalen Wert an). Sie können die auf der Schaltfläche angezeigte Aktion einzeln anwenden, ohne die übrigen Bedrohungen zu neutralisieren. Klicken Sie dazu hier.
Pfad	In dieser Spalte wird der vollständige Pfad der entsprechenden Datei angegeben.

Wenn Sie in den **Dr.Web Scanner** Einstellungen das Kontrollkästchen **Aktionen für Bedrohungen automatisch verwenden** aktiviert haben, werden die Bedrohungen automatisch neutralisiert.

6.3. Scanner konfigurieren

Bei der Nutzung des Programms unter den Betriebsystemen Windows Vista, Windows Server 2003 und späteren Versionen wird es empfohlen, den **Dr.Web Scanner** mit Administratorrechten zu starten.

Die Default-Einstellungen sind für die meisten Anwendungen des **Dr.Web Scanners** optimal und sollen nur im Notfall geändert werden.

Einstellungen des Dr.Web Scanners ändern

1. Im Menü des **SpIDer Agenten** wählen Sie den Punkt **Scanner.** Es öffnet sich das Menü für den Schnellzugriff auf die Scanmodi.
2. Wählen Sie den Punkt **Benutzerdefiniert**. Es öffnet sich das Hauptfenster des **Dr.Web Scanners**. Punkte **Schnell** und **Vollständig** starten entsprechende Scanvorgänge (Die Scan-Einstellungen werden dabei unzugänglich sein, bis der Scanvorgang abgeschlossen oder unterbrochen wird).
3. Klicken Sie in der Symbolleiste auf das Symbol der Einstellungen .

   Die Grundeinstellungen können erst dann geändert werden, wenn diese Aktion vom Administrator des Zentralschutz-Servers, mit dem sich **Dr.Web** verbindet, zugelassen wurde.

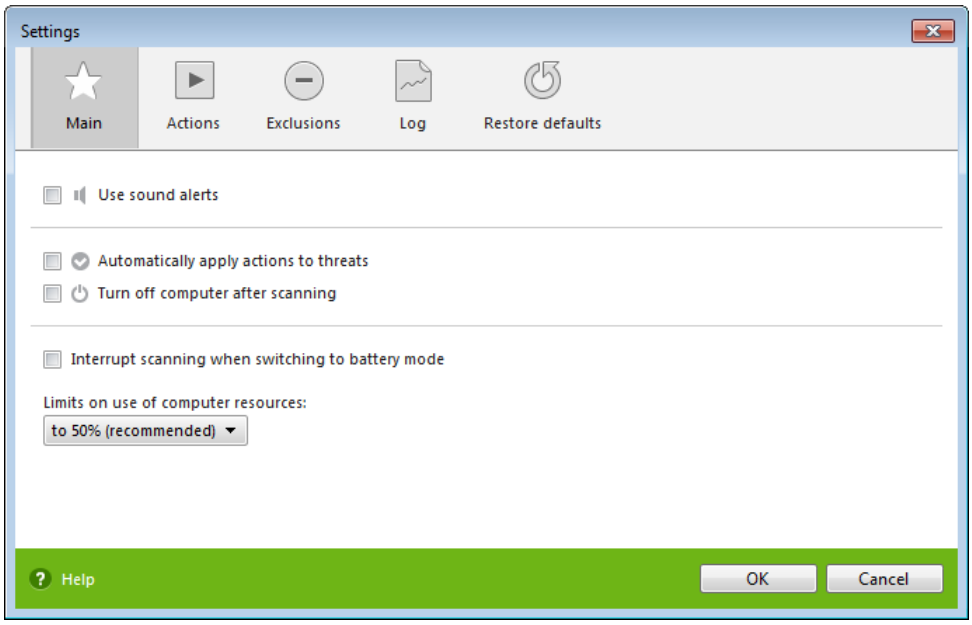
   In Es öffnet sich das Fenster mit Einstellungen, das die folgenden Tabs enthält:

   - Tab Grundeinstellungen, in dem allgemeine Parameter des **Dr.Web Scanners** konfiguriert werden;
   - Tab Aktionen, in dem die Reaktion des **Dr.Web Scanners** bei Erkennung infizierter und verdächtiger Dateien sowie Schadprogramme eingestellt wird;
   - Tab Ausnahmen, in dem zusätzliche Einschränkungen zur Prüfung der Dateien festgelegt werden;
   - Tab Bericht, in dem Protokollierungsmodus des **Dr.Web Scanners** konfiguriert wird;
   - Tab Einstellungen rücksetzen, in dem der Benutzer die Default-Einstellungen des **Dr.Web Scanners** wiederherstellen kann.

4. Um detaillierte Informationen zu den jeweils konfigurierbaren Einstellungen zu erhalten, klicken Sie auf **Hilfe** .
5. Nachdem Sie die Einstellungen bearbeitet haben, klicken Sie auf den **OK**, um vorgenommene Änderungen zu speichern, oder auf den **Abbrechen**, um die Änderungen zu verwerfen.

Grundeinstellungen

In diesem Tab werden die Grundparameter des **Dr.Web Scanners** konfiguriert.



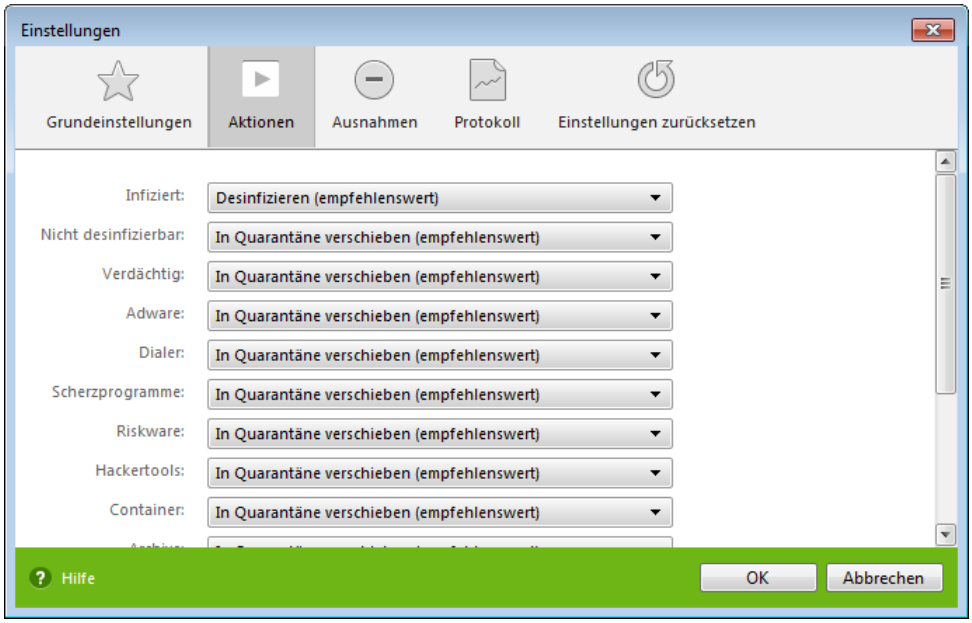
Einstellung	Beschreibung
Tonbegleitung der Ereignisse	Markieren Sie das Kontrollkästchen, damit **Dr.Web Scanner** jedes Ereignis mit einem Audiosignal begleitet.
Aktionen für Bedrohungen automatisch verwenden	Aktivieren Sie dieses Kontrollkästchen, damit der **Dr.Web Scanner** automatisch Aktionen für die erkannten Bedrohungen anwendet.
Den Computer nach dem Beenden der Prüfung herunterfahren	Markieren Sie das Kontrollkästchen, damit der Computer nach Abschluss der Überprüfung heruntergefahren wird. Ist dabei das Kontrollkästchen **Aktionen für Bedrohungen automatisch verwenden** aktiviert, wird **Dr.Web Scanner** die definierten Aktionen für die erkannten Bedrohungen verwenden, bevor der Computer heruntergefahren wird.
Prüfung beim Wechsel zur Batteriespeisung abbrechen	Markieren Sie das Kontrollkästchen, um die Überprüfung beim Wechsel zum Batteriebetrieb abzubrechen.
Maximal erlaubte CPU-Auslastung	Diese Option bestimmt eine maximal erlaubte CPU-Auslastung **Scanner Dr.Web**. Der Standardwert beträgt 50%.

Die Parameter **Tonbegleitung der Ereignisse**, **Aktionen für Bedrohungen automatisch verwenden** und **Den Computer nach dem Beenden der Prüfung herunterfahren** können ebenso schnell im Hauptfenster von **Dr.Web Scanner** bzw. im Fenster für benutzerdefinierte Auswahl konfiguriert werden. Klicken Sie dazu auf das Symbol in der Toolbar.

Aktionen

Neutralisierung konfigurieren

1. Wechseln Sie zum Bereich **Aktionen**.



2. In der Dropdown-Liste **Infiziert** wählen Sie die Reaktion des **Scanners** beim Fund eines infizierten Objektes aus.

   Der optimale Wert ist **Desinfizieren**.

3. In der Dropdown-Liste **Nicht desinfizierbar** wählen Sie die Reaktion des **Scanners** beim Fund eines nicht desinfizierbaren Objektes aus. Diese Aktion ist der im Punkt oben beschriebenen Aktion ähnlich, es aber fehlt die Option **Desinfizieren**.

   Meistens ist die Variante **In Quarantäne verschieben** optimal.

4. In der Dropdown-Liste **Verdächtig** wählen Sie die Reaktion des **Scanners** beim Fund eines verdächtigen Objektes aus (identisch dem Punkt oben).
5. Die Reaktion des **Scanners** beim Fund der Objekte, die Adware, Dialers, Scherzprogramme, Riskware bzw. Hacktools enthalten, wird ähnlicherweise eingestellt.
6. Ähnlich werden die automatischen Aktionen des **Scanners** beim Fund von Viren oder einem verdächtigen Code in den Archiven, Container-Dateien und Postfächern eingestellt. Die Aktionen für oben genannte Objekte werden in Bezug nicht auf den infizierten Teil, sondern auf das ganze Objekt ausgeführt.
7. Das erfolgreiche Desinfizieren mancher infizierten Dateien benötigt einen Neustart des Betriebssystems. Sie können zwischen folgenden Varianten auswählen:
   - **Neustart anbieten**;
   - **Computer automatisch neu starten.** In diesem Modus können die nicht gespeicherten Daten verloren gehen.

Die optimale Reaktion auf erkannte desinfizierbare Bedrohungen (z. B. mit Viren infizierte Dateien) ist Desinfizieren, bei dem der ursprüngliche Zustand des Objekts vor der Infizierung wiederhergestellt wird.

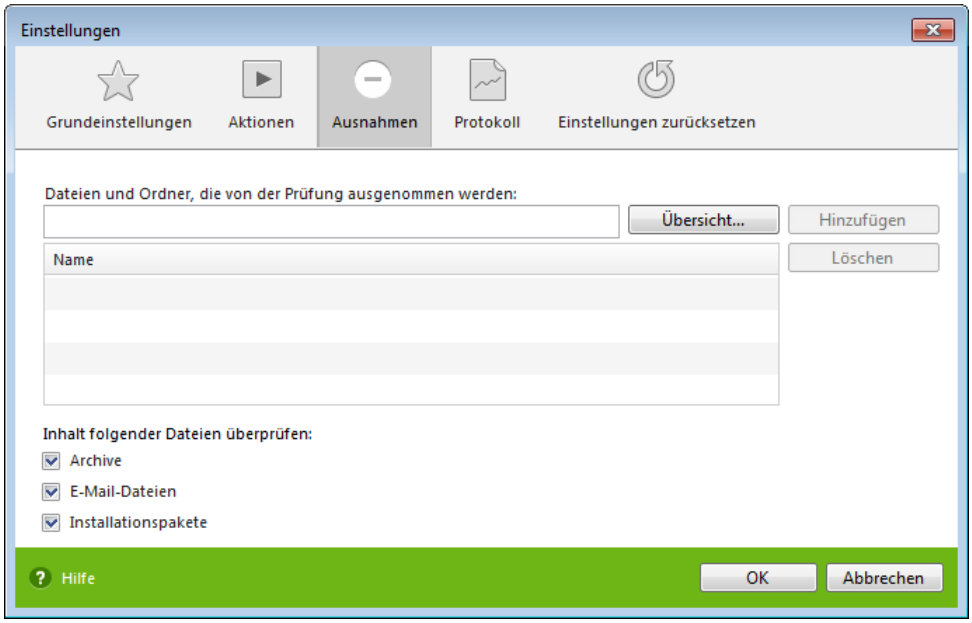
Es wird empfohlen, Bedrohungen anderer Art in die Quarantäne zu verschieben und dadurch zufälligen Verlust der wertvollen Daten zu verhindern. Sie können zwischen folgenden Reaktionen auswählen:

Aktion	Beschreibung
Desinfizieren	Das Objekt wird in seinem Stand vor Infizierung wiederhergestellt. Sollte das Virus undesinfizierbar sein oder der Desinfizierungsversuch fehlgeschlagen ist, wird eine vordefinierte Aktion für die nicht desinfizierbaren Viren vorgenommen. Ausführung dieser Aktion ist nur für Objekte möglich, die von einem bekannten desinfizierbaren Virus infiziert sind, außer Trojaner und infizierter Dateien innerhalb von zusammengesetzten Objekten (Archive, E-Mail-Dateien bzw. Container-Dateien). Die Trojaner werden bei Entdeckung gelöscht. Darüber hinaus ist es die einzige Aktion, die für infizierte Bootsektoren zugänglich ist.
In Quarantäne verschieben	Objekt in ein spezielles Verzeichnis zur Isolierung verschieben. Für die Bootsektoren werden keine Aktionen durchgeführt.
Löschen	Das Objekt wird aus dem System vollständig gelöscht. Für die Bootsektoren werden keine Aktionen durchgeführt.
Überspringen	Das Objekt wird übersprungen. Dabei werden keine Aktionen vorgenommen und keine Infos protokolliert. Diese Aktion ist nur für schädliche Programme möglich: Adware, Dialer, Scherzprogramme, Riskware und Hacktools.

Beim Erkennen der Viren bzw. eines verdächtigen Codes innerhalb der zusammengesetzten Objekte (Archive, E-Mail-Dateien bzw. Container-Dateien) werden Aktionen für die Bedrohungen innerhalb solcher Objekte für das ganze Objekt verwendet und nicht nur für infizierten Bestandteil des Objekts.

Ausnahmen

Auf dieser Registerkarte werden zusätzliche Einschränkungen in Bezug auf den Bestand der durchsuchten Dateien festgelegt.



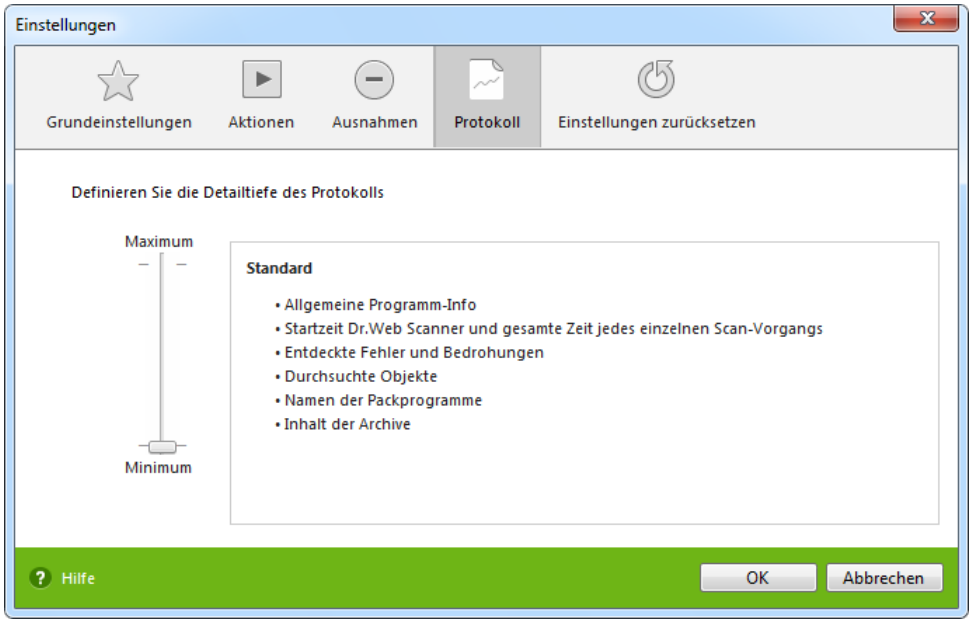
Hier können Sie die Liste der Dateien (Masken der Dateien), die nicht gescannt werden, festlegen (von der Prüfung werden alle Dateien mit einem solchen Namen ausgenommen). Dies können temporäre Dateien (Swap-Dateien) u a.m. sein.

Sie können auch angeben, ob der Inhalt von Archiven, E-Mails bzw. Installationspaketen überprüft werden soll.

Protokoll

Auf dieser Registerkarte können Sie die Parameter für die Protokollführung konfigurieren.

Das Protokoll von **Dr.Web Scanner** wird in der Datei dwscanner.log gespeichert, die sich im Verzeichnis %USERPROFILE%\Doctor Web befindet. Es wird empfohlen, eine regelmäßige Analyse der Protokolldatei durchzuführen.



Die meisten Standardeinstellungen sollten protokolliert werden. Sie können aber die Detailstufe der Protokollierung individuell anpassen. Das Protokoll enthält immer Informationen zu infizierten und verdächtigen Objekten. Statistiken zu archivierten Dateien und Archiven sowie zur erfolgreichen Prüfung anderer Dateien werden standardmäßig nicht protokolliert.

Sie können zwischen folgenden Detailtiefen des Berichts auswählen:

- **Standartd –** in diesem Modus erfasst das Protokoll nur die wichtigsten Ereignisse, wie Aktualisierung, Starten und Beenden des **Dr.Web Scanners**, die erkannten Bedrohungen sowie Angaben über die Namen der Packprogramme und den Inhalt von gescannten Archiven. Bei Bedarf können Sie solche Objekte auch in die Liste der Ausnahmen hinzufügen, was die Auslastung des Systems reduzieren kann Dieser Modus ist optimal in den meisten Fällen;
- **Debug –** in diesem Protokollmodus wird die maximale Informationsmenge über den Betrieb des **Dr.Web Scanners** festgehalten, was zu einer erheblichen Vergrößerung der Protokolldatei führen kann. Die Nutzung dieses Modus wird nur bei Schwierigkeiten im Betrieb des **Dr.Web Scanners** oder auf Bitte des Administrators Ihres Antivirus-Netzwerks empfohlen.

Für den **Standard-Modus** beträgt die erlaubte Protokolldateigröße 10 MB. Die Dateigröße im Debugging-Modus ist nicht eingeschränkt.

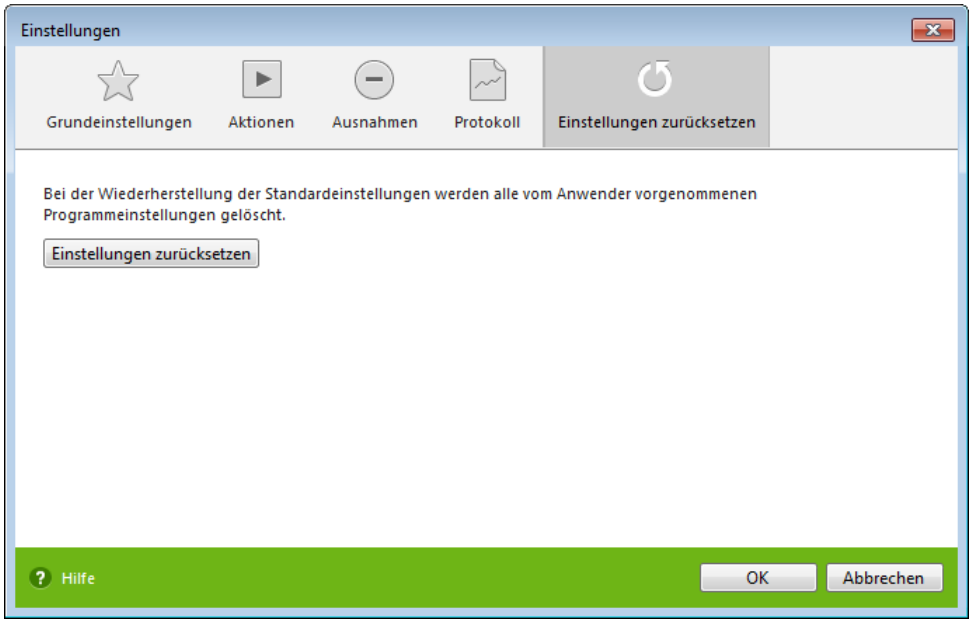
Wenn die maximale Größe der Protokolldatei überschritten wurde, wird sie nach Abschluss der Überprüfung reduziert auf:

- festgelegte Größe, wenn die während der Sitzung gespeicherten Daten die erlaubte Größe nicht übersteigen;
- die Größe der laufenden Sitzung, wenn die während der Sitzung gespeicherten Daten die erlaubte Größe übersteigen (auf diese Weise werden die Daten bis zum Start der nächsten Überprüfung gespeichert).

Beim Start der Überprüfung wird die Protokolldatei auf die durch die Einstellungen vorgegebene Größe reduziert.

Einstellungen zurücksetzen

Im Bereich zur Wiederherstellung der Einstellungen können Sie die Einstellungen vom **Dr.Web Scanner** wiederherstellen. Klicken Sie dafür auf **Einstellungen zurücksetzen**.



6.4. Scanner mit Befehlszeilenparametern starten

Sie können den **Dr.Web Scanner** im Befehlszeilenmodus starten. Mit einem solchen Verfahren lassen sich die Einstellungen der aktuellen Scan-Sitzung sowie die Liste der zu scannenden Objekte als Aufrufeparameter konfigurieren.

Scanner über Befehlszeile starten

Um den **Scanner** mit den zusätzlichen Befehlszeilenparametern zu starten, führen Sie den folgenden Befehls aus:

[*<Pfad_des_Programms>*]`dwscanner` [*<Schlüssel>*] [*<Objekte>*]

wobei:

- *<Objekte>* – Liste der zu scannenden Objekte;
- *<Schalter>* sind Befehlszeilenparameter, welche die Einstellungen des **Scanners** definieren. Wenn diese Parameter fehlen, wird die Überprüfung anhand der vorher gespeicherten Einstellungen (bzw. der Standardeinstellungen, wenn sie nicht geändert wurden) durchgeführt.

Die Liste der Objekte kann leer sein oder mehrere durch Leerzeichen getrennte Elemente enthalten. Die meist verwendeten Scanmodi sind:

- `/FAST` – schnelle Prüfung des Systems ausführen.
- `/FULL` – vollständige Prüfung aller Festplatten und Wechseldatenträger (einschließlich Bootsektoren) ausführen.
- `/LITE` – Startprüfung des Systems ausführen. Dabei werden der Hauptspeicher, die Bootsektoren aller Laufwerke gescannt sowie die Prüfung auf das Vorhandensein von Rootkits ausgeführt.

Parameter sind Befehlszeilenschalter, welche die Einstellungen des Programms definieren. Wenn diese Parameter fehlen, wird die Überprüfung mit den vorher gespeicherten Einstellungen (bzw. mit den Standardeinstellungen, wenn diese von Ihnen nicht geändert wurden) durchgeführt. Die Schlüssel werden mit dem „/" Zeichen angefangen und, wie auch alle anderen Befehlszeilenparameter, mit Leerzeichen getrennt.

6.5. Konsolen-Scanner

Zum Leistungsumfang von **Dr.Web** gehört auch der **Konsolen-Scanner**, der die Prüfung im Befehlszeilenmodus ermöglicht sowie mehrere Einstellungsmöglichkeiten bietet.

Die Dateien mit Verdacht auf schädliche Objekte werden vom **Konsolen-Scanner** in die **Quarantäne** verschoben.

Konsolen-Scanner starten

Um den **Konsolen-Scanner** zu starten, benutzen Sie folgenden Befehl:

[*<Pfad_zum_Programm>*]`dwscancl` [*<Schalter>*] [*<Objekte>*]

wobei:

- *<Objekte>* – Liste der zu scannenden Objekte;
- *<Schalter>* – Liste der Befehlszeilenparameter, welche die Einstellungen des **Konsolen-Scanners** bestimmen.

Der Schlüssell beginnt mit dem „/" Zeichen. Mehrere Schlüssell werden mit Leerzeichen getrennt. Die Liste der Scan-Objekte kann entweder leer sein oder manche mit Leerzeichen getrennte Elemente enthalten.

Die Liste der Schlüssel für **Konsolen-Scanner** finden Sie im Anhang A.

Nach der Ausführung gibt der **Konsolen-Scanner** einen der folgenden Rückgabecodes aus:

0 – Scannen erfolgreich abgeschlossen, keine infizierten Objekte gefunden;
1 – Scanvorgang erfolgreich abgeschlossen, infizierte Objekte gefunden;
10 – ungültige Schalter angegeben;
11 – Schlüsseldatei nicht gefunden oder unterstützt den **Konsolen-Scanner** nicht;
12 – **Scanning Engine** nicht gestartet;
255 – Scanvorgang durch Benutzer abgebrochen.

6.6. Überprüfung nach Zeitplan starten

Bei der Installation von **Dr.Web** wird im standardmäßigen Windows-Aufgabenplaner die Aufgabe zur Durchführung der Virenprüfung (standardmäßig ist sie deaktiviert) automatisch erstellt.

Um die Parameter der Aufgabe einzusehen, navigieren Sie zu **Systemsteuerung** (erweiterte Ansicht) → **Verwaltung** → **Aufgabenplanung.**

In der Aufgabenliste wählen Sie die Aufgabe zur Virenprüfung aus. Sie können die Aufgabe aktivieren sowie die Uhrzeit für den Start der Überprüfung eingeben und benötigte Parameter definieren.

Im unteren Fensterbereich auf der Registerkarte **Allgemein** werden allgemeine Daten zu Aufgabe sowie die Sicherheitsoptionen angegeben. Auf den Registerkarten **Trigger** und **Bedingungen** werden unterschiedliche Bedingungen angegeben, unter welchen die Aufgabe gestartet wird. Die Ereignishistorie kann man sich auf der Registerkarte **Verlauf** ansehen.

Sie können unter anderem eigene Aufgaben zur Virenprüfung erstellen. Mehr zur Nutzung des Zeitplans finden Sie in der Online-Hilfe bzw. in der Windows-Begleitdokumentation.

Gehört die Firewall zu den installierten Komponenten, wird der Windows-Aufgabenplaner nach der Installation von **Dr.Web** und dem ersten Neustart durch die **Firewall** gesperrt. Die Komponente **Geplante Aufgaben** wird erst nach dem erneuten Neustart funktionsfähig, da die benötigte Regel zu dem Zeitpunkt bereits erstellt wird.

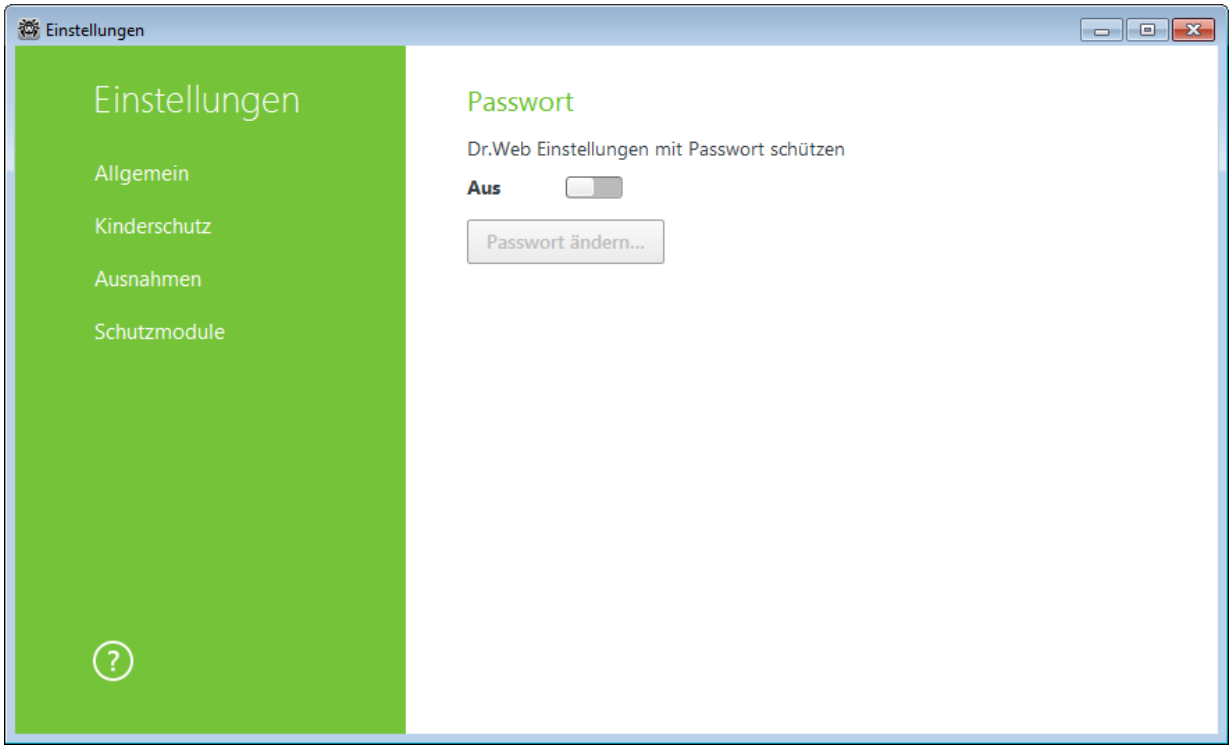
7. Einstellungen

Die Einstellungen sind in dem Benutzermodus nicht abrufbar.

Passwortschutz

Um den Zugriff auf die Einstellungen von **Dr.Web** auf Ihrem Computer einzuschränken, aktivieren Sie die Option **Dr.Web Einstellungen mit Passwort schützen**. Im geöffneten Fenster geben Sie ein Passwort ein, das bei Abruf der Einstellungen von **Dr.Web** abgefragt wird, bestätigen Sie das eingegebene Passwort und klicken auf **OK.**

Sollten Sie das Passwort für Produkteinstellungen vergessen haben, kontaktieren Sie bitte den Administrator Ihres Antivirus-Netzwerks.



8. Allgemeine Einstellungen

Die Grundeinstellungen können geändert werden, wenn es vom Administrator des zentral verwalteten Virenschutz-Servers, zu dem **Dr.Web** die Verbindung herstellt, erlaubt ist.

Um die Grundeinstellungen von **Dr.Web** ändern zu können, müssen Sie jedesmal das ensprechende Passwort angeben, wenn Sie im Bereich Einstellungen die Option **Dr.Web Eistellungen mit Passwort schützen** aktiviert haben.

Die Einstellungen von **Dr.Web** sind in dem Benutzermodus nicht abrufbar.

Das einheitliche Verwaltungscenter ermöglicht es, die allgemeinen Einstellungen des Antivirus-Systems zu konfigurieren.

8.1. Benachrichtigungen

In diesem Bereich können Sie den Typ der Hinweise bzw. Benachrichtigungen festlegen, als Popup-Fenster über dem Symbol **SpIDer Agent** im Windows-Infobereich erscheinen.

Benachrichtigungen auf dem Bildschirm anzeigen

Aktivieren Sie diese Option, um Benachrichtigungen als Popupfenster oberhalb des Symbols **SpIDer Agent** in dem Windows-Infobereich angezeigt zu bekommen.

Benachrichtigungs-Parameter

1. Klicken Sie auf **Benachrichtigungs-Parameter**.
2. Wählen Sie die Benachrichtigungen aus, die Sie erhalten wollen. Aktivieren Sie dafür die entsprechenden Kontrollkästchen.
3. Legen Sie bei Bedarf zusätzliche Einstellungen für die Anzeige der Desktop-Benachrichtigungen fest:

Kontrollkästchen	Beschreibung
Benachrichtigung nicht im Vollbildmodus anzeigen	Aktivieren Sie diese Option, damit keine Benachrichtigungen bei der Arbeit mit Programmen im Vollbildmodus (beim Abspielen von Videos, Anzeigen von Bildern usw.) angezeigt werden. Deaktivieren Sie dieses Kontrollkästchen, um Benachrichtigungen immer zu erhalten.
Benachrichtigungen der Firewall im separaten Fenster im Vollbildmodus anzeigen	Aktivieren Sie dieses Kontrollkästchen, damit **Firewall**-Benachrichtigungen als separates Fenster bei der Arbeit mit Vollbild-Programmen (Spiele, Videos) angezeigt werden. Wenn diese Option deaktiviert ist, werden Benachrichtigungen im gleichen Fenster angezeigt, in dem ein Programm im Vollbildmodus ausgeführt wird.

Nachdem Sie die Einstellungen bearbeitet haben, klicken Sie auf den **OK**, um vorgenommene Änderungen zu speichern, oder auf den **Abbrechen**, um die Änderungen zu verwerfen.

Typ der Benachrichtigung	Beschreibung
Benachrichtigungen über Bedrohungen	Aktivieren Sie das Kontrollkästchen, um Benachrichtigungen über erkannte Bedrohungen zu erhalten. Deaktivieren Sie das Kontrollkästchen, um diese Benachrichtigungen nicht zu erhalten. Standardmäßig ist diese Option aktiviert.
Wichtige Benachrichtigungen	Aktivieren Sie das Kontrollkästchen, um folgende wichtige Benachrichtigungen zu erhalten: • Computer-Sitzung ist abgelaufen, • Zugriffsversuche auf das geschützte Objekt bzw. Versuche, das Systemdatum zu ändern, wurden gesperrt, • Virendatenbanken sind veraltet (im Mobilmodus). Deaktivieren Sie das Kontrollkästchen, um diese Benachrichtigungen nicht zu erhalten. Standardmäßig ist diese Option aktiviert.
Kritische Benachrichtigungen	Aktivieren Sie das Kontrollkästchen, um folgende kritische Benachrichtigungen zu erhalten:, • eine Verbindung wartet auf die Antwort von der **Firewall**, • Ihr Benutzername und Passwort werden für die Verbindung mit dem Zentralschutz-Server bereits verwendet. Deaktivieren Sie das Kontrollkästchen, um diese Benachrichtigungen nicht zu erhalten. Standardmäßig ist diese Option aktiviert.
Geringfügige Benachrichtigungen	Aktivieren Sie das Kontrollkästchen, um folgende geringfügige Benachrichtigungen zu erhalten: • Aktualisierung ist erfolgreich abgeschlossen, • Aktualisierung ist fehlgeschlagen, • Internet-Sitzung ist abgelaufen, • eine bestimmte URL wurde gesperrt, • ein Zugriffsversuch auf das geschützte Objekt wurde gesperrt, • Administrator des Antivirus-Netzwerks hat Ihren Rechner scannen lassen, • Zeitgesteuerte Prüfung Ihres Rechners wird momentan ausgeführt, • Überprüfung Ihres Rechners ist abgeschlossen. Deaktivieren Sie das Kontrollkästchen, um diese Benachrichtigungen nicht zu erhalten. Standardmäßig ist diese Option deaktiviert.

Benachrichtigungen über einige Ereignisse gehören nicht den oben aufgeführten Gruppen und werden dem Benutzer immer angezeigt:

- Installation vorrangiger Updates, die einen Neustart erfordern;
- Aufforderung zur Bestätigung, wenn ein Prozess ein Objekt zu modifizieren versucht;
- Benachrichtigung, die vom Administrator des Zentralschutz-Server gesendet wurde.

8.2. Selbstschutz

In diesem Bereich können Sie die Parameter für den Selbstschutz von **Dr.Web** vor unerlaubten Einwirkungen von z. B. Antivirus-Programmen sowie der zufälligen Beschädigung konfigurieren.

Die Option **Selbstschutz aktivieren** erlaubt es, Dateien und Prozesse von **Dr.Web** vor dem unerlaubten Zugriff zu schützen. Es wird nicht empfohlen, den Selbstschutz zu deaktivieren.

Falls Probleme bei Nutzung der Defragmentierungsprogramme entstehen, ist es empfehlenswert, den Selbstschutz temporär zu deaktivieren.

Um zu dem Systemwiederherstellungspunkt zurück zu kehren, sollte der Selbstschutz deaktiviert werden.

Die Option **Emulation von Benutzer-Aktionen sperren** erlaubt es, jeglichen Änderungen in der Funktion von **Dr.Web**, die automatisch veranlasst werden, vorzubeugen. Darunter wird die Ausführung der Skripte verboten, die Verwendung von **Dr.Web** durch Benutzer emulieren und vom Benutzer selbst gestartet wurden.

Die Option **Ändern des Systemdatums bzw. der Systemzeit verbieten** erlaubt es, die manuelle bzw. automatische Änderung des Systemdatums und der Systemzeit sowie der Zeitzone zu blockieren. Diese Einschränkung gilt für alle Benutzer des Systems. Diese Einstellung lässt die Zeitbeschränkung in **Office Control** besser funktionieren. Wenn die Computer- bzw. Internetnutzung durch **Office Control** beschränkt wird, wird diese Einstellung automatisch aktiv. Sie können das Erhalten von Benachrichtigungen für den Fall konfigurieren, dass es versucht wird, die Systemzeit zu ändern.

8.3. Endgeräte

Die Einstellungen für die Zugangskontrolle werden für alle Windows-Benutzerkonten verwendet.

Endgeräte

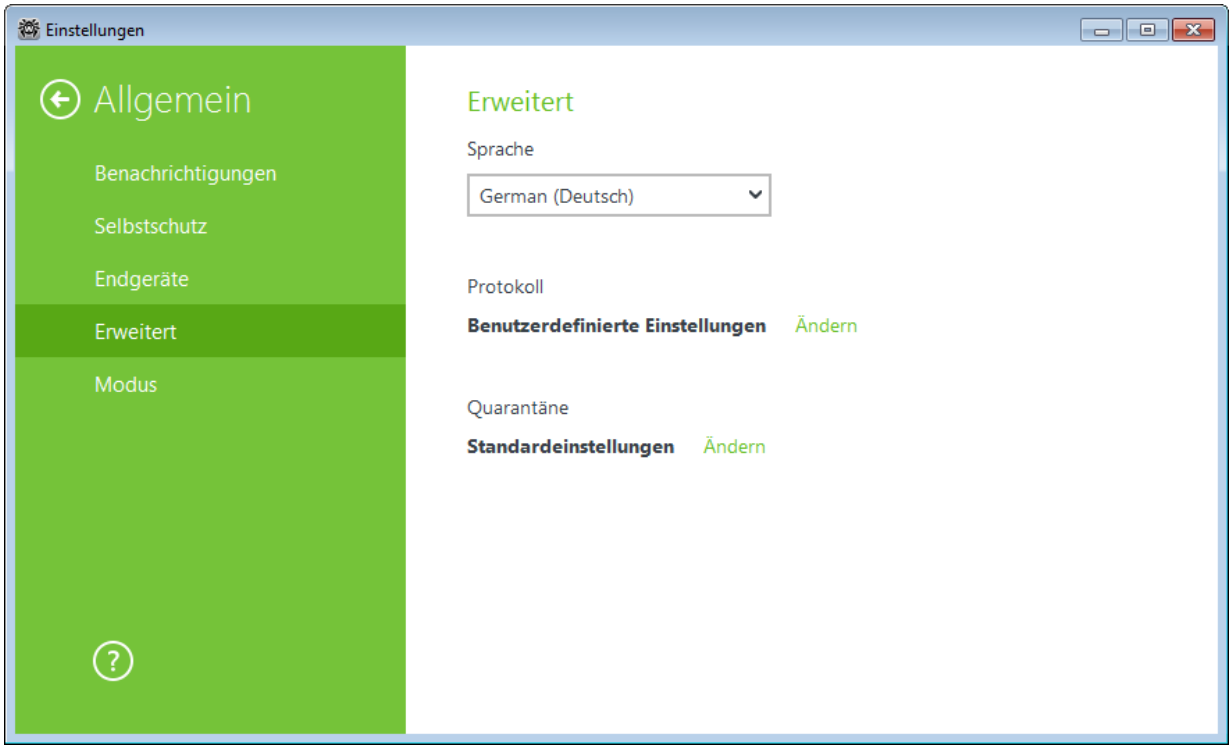
Um den Zugriff auf die auf Wechseldatenträgern (USB-Massenspeichern, Disketten, CD/DVD-Laufwerken, ZIP-Laufwerken usw.) gespeicherten Daten zu verbieten, aktivieren Sie die entsprechende Option. Um das Senden der Druckaufträge an den Drucker zu verbieten, setzen Sie das Häkchen bei **Senden der Aufträge an den Drucker blockieren.** Standardmäßig ist diese Option deaktiviert. Sie haben auch die Möglichkeit, die Datenvermittlung über lokale Netzwerke und das Internet zu verbieten.

Endgeräteklassen und Busse

Um den Zugriff auf bestimmte Endgeräteklassen und Busse zu sperren, aktivieren Sie die entsprechenden Optionen. Sie können eine Liste mit solchen Objekten zusammenstellen, indem Sie auf **Ändern** klicken.

8.4. Erweitert

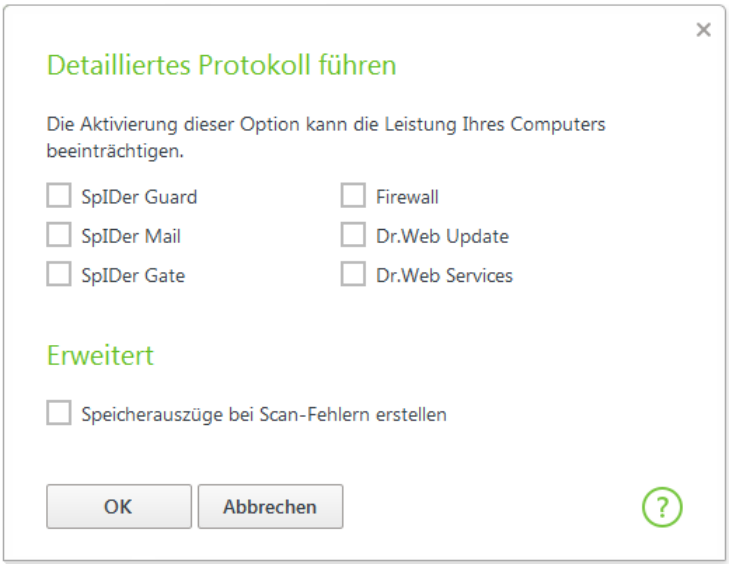
In diesem Abschnitt können Sie zusätzliche Einstellungen des Antivirenschutzes festlegen.



Sie können die Sprache des Programms in der Dropdown-Liste auswählen. Die Liste der Sprachen wird automatisch aktualisiert und enthält alle zu dem aktuellen Zeitpunkt verfügbaren Lokalisierungen der grafischen Benutzeroberfläche von **Dr.Web**.

Protokolleinstellungen

Um die Einstellungen des Protokollierens zu verwalten, klicken Sie auf **Ändern**.



Es ist nicht möglich, die Einstellungen für die Protokollführung zu ändern, wenn diese Aktion durch den Administrator des zentral verwalteten Virenschutz-Servers, mit dem **Dr.Web** verbunden wird, nicht erlaubt wurde.

\

Standardmäßig ist die Größe einer Protokolldateien auf 10 MB begrenzt.Wenn die maximale Größe der Protokolldatei überschritten wird, wird sie reduziert auf:

- die festgelegte Größe, wenn die während der Sitzung gespeicherten Daten die erlaubte Größe nicht übersteigen;
- die Größe der laufenden Sitzung, wenn die während der Sitzung gespeicherten Daten die erlaubte Größe übersteigen.

Bei Standardeinstellungen werden Protokolle für alle Komponenten von **Dr.Web** im Standard-Modus geführt, in dem die folgenden Informationen gespeichert werden:

Komponente	Informationen
SpIDer Guard	Aktualisierung, Starten und Anhalten von **SpIDer Guard**, Virenereignisse, Daten über die durchsuchten Dateien, Namen der Packprogramme und Inhalte der durchsuchten zusammengesetzten Objekte (Archive, E-Mail-Dateien bzw. Container-Dateien). Es wird empfohlen, diesen Modus zur Erkennung der Objekte zu verwenden, die von **SpIDer Guard** besonders häufig durchsucht werden. Bei Bedarf können Sie solche Objekte der Liste von Ausnahmen hinzufügen, wodurch die Beanspruchung des Computers reduziert werden kann.
SpIDer Mail	Aktualisierung, Starten und Anhalten von **SpIDer Mail**, Virenereignisse, Parameter für das Abfangen von Verbindungen sowie Daten zu den durchsuchten Dateien, Namen der Packprogramme und Inhalten der durchsuchten Archive. Es wird empfohlen, diesen Modus zur Prüfung der Einstellungen für das Abfangen von Verbindungen mit Mail-Servern zu verwenden.
SpIDer Gate	Aktualisierung, Starten und Anhalten von **SpIDer Gate**, Virenereignisse, Parameter für das Abfangen von Verbindungen sowie Daten zu den durchsuchten Dateien, Namen der Packprogramme und Inhalten der durchsuchten Archive. Es wird empfohlen, diesen Modus zur Gewinnung detaillierter Informationen zu den durchsuchten Objekten und der Funktion des Web-Antivirus-Moduls zu verwenden.
Firewall	Bei Standardeinstellungen wird keine Protokolldatei der **Firewall** geführt. Bei der Aktivierung des Modus für detaillierte Protokollführung werden die Daten über Netzwerk-Pakete (pcap-Logs) gesammelt.
Dr.Web Update	Die Liste der aktualisierten Dateien von **Dr.Web** sowie deren Download-Status, Informationen über die Funktion der unterstützenden Skripte, Datum und Uhrzeit der Aktualisierung, Informationen über den Neustart der Komponenten von **Dr.Web** nach der Aktualisierung.
Dienste Dr.Web	Informationen über die Komponenten von **Dr.Web**, die Änderung der Einstellungen der Komponenten, Aktivieren bzw. Deaktivieren von Komponenten, Ereignisse des Präventivschutzes, Verbindungsaufbau zum zentral verwalteten Virenschutz-Server.

Speicherauszüge erstellen

Die Option **Speicherauszüge bei Scan-Fehlern erstellen** erlaubt es, die maximale Menge an Informationen über die Ursachen der fehlerhaften Funktion der Komponenten von **Dr.Web** zu speichern, was den Spezialisten von **Doctor Web** ermöglicht, im Weiteren eine umfangreichere Analyse des Problems durchzuführen und eine Lösung anzubieten. Es wird empfohlen, diese Option nur bei eventuellen Fehlern bei der Dateiprüfung bzw. Neutralisierung von Bedrohungen oder auf die Bitte der Spezialisten von **Dr.Web** zu aktivieren. Das Speicherabbild wird als DMP-Datei im Verzeichnis %PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\ abgespeichert.

Detaillierte Protokollführung aktivieren

Bei der detaillierten Protokollführung wird die maximale Informationsmenge über die Funktionsweise der Komponenten von **Dr.Web** gespeichert. Dadurch wird die Beschränkung für die maximale Größe von Protokolldateien außer Kraft gesetzt und die Leistung von **Dr.Web** und des Betriebssystems beeinträchtigt. Sie sollten diesen Modus nur dann verwenden, wenn Probleme im Betrieb der Komponenten auftreten bzw. wenn Sie vom Administrator Ihres Antivirus-Netzwerks darum gebeten werden.

1. Um die detaillierte Protokollführung für eine der Komponenten von **Dr.Web** zu aktivieren, aktivieren Sie das entsprechende Kontrollkästchen.
2. Speichern Sie die Änderungen.

Quarantäne-Eigenschaften

Um die Einstellungen der Quarantäne zu verwalten, klicken Sie auf **Ändern**.

Sie können die Funktionsparameter der **Dr.Web** Quarantäne konfigurieren, ihre Größe analysieren sowie alle isolierten Dateien von einem bestimmten Laufwerk löschen.

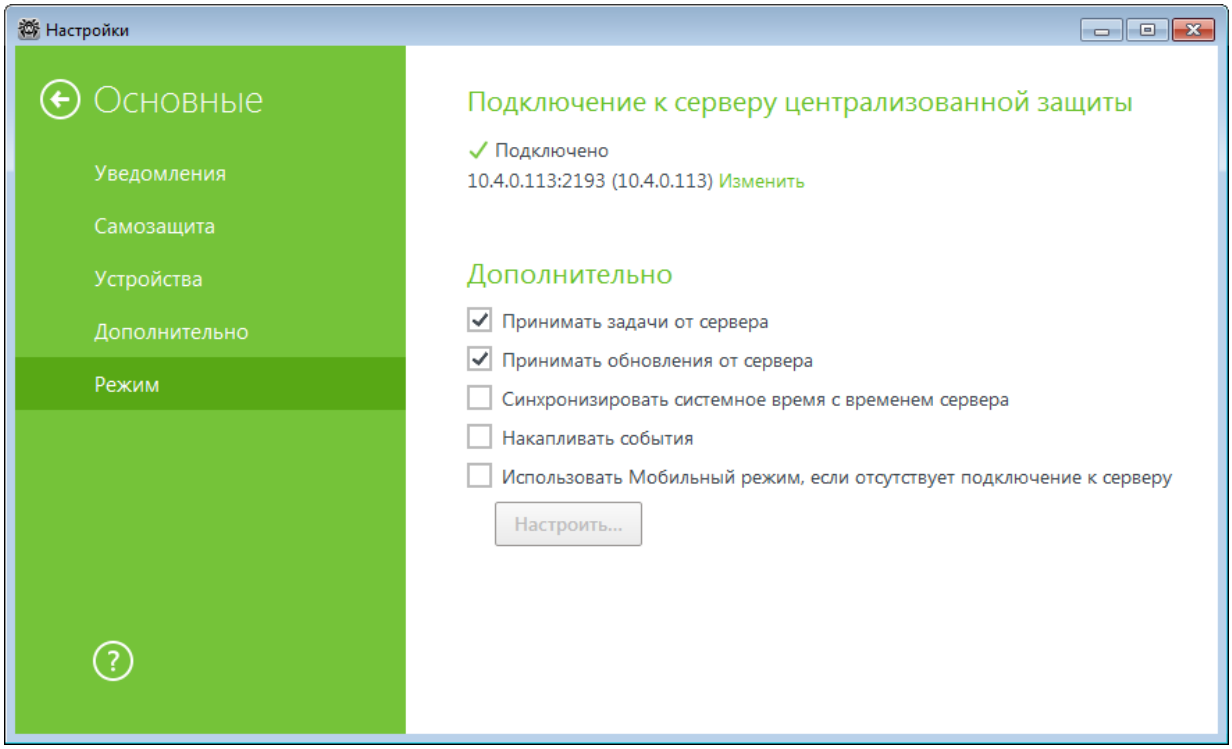
Das Quarantäne-Verzeichnis wird auf jedem logischen Laufwerk, auf welchem verdächtige Dateien entdeckt wurden, gesondert erstellt.

Quarantäne leeren

1. Um alle Dateien im Quarantäne-Verzeichnis auf einem bestimmten Laufwerk zu löschen, wählen Sie dieses Laufwerk in der Liste aus.
2. Um alle Dateien im **Quarantäne**-Verzeichnis auf einem bestimmten Laufwerk zu löschen, wählen Sie dieses Laufwerk in der Liste aus.
3. Klicken Sie auf **Leeren** und bestätigen Sie den Löschvorgang.

8.5. Modus

In diesem Abschnitt können Sie die Parameter für die Kommunikation von **Dr.Web** mit dem zentral verwalteten Virenschutz-Server einsehen und bearbeiten sowie die Einstellungen für den Mobilmodus von **Dr.Web** festlegen. Die Änderung der Kommunikationsparameter mit Server kann von dem Administrator Ihres Antivirus-Netzwerks verboten sein. In diesem Fall sind die Buttons und Kontrollkästchen nicht zugänglich.



In der Gruppe **Verbindung zum zentral verwalteten Virenschutz-Server** wird der **Verbindungsstatus** angezeigt. Hier können Sie auch die Verbindungseinstellungen zum Server einsehen und bearbeiten, vorausgesetzt, dass Sie über entsprechende Rechte verfügen.

Die Änderung der Verbindungseinstellungen zum zentral verwalteten Virenschutz-Server muss mit dem Administrator des Antivirus-Netzwerks abgestimmt werden. Im Gegenfall wird Ihr Computer vom Antivirus-Netzwerk getrennt.

Um die Einstellungen für die Verbindung mit dem aktuellen Server zu ändern bzw. eine Verbindung mit einem anderen Server herzustellen, klicken Sie auf **Ändern.** Es öffnet sich dabei das Fenster **Server-Einstellungen**.

Gegebenenfalls können Sie die Parameter ändern:

- **Adresse** und **Port –** geben Sie die Adresse und den Port des zentral verwalteten Virenschutz-Servers an.
- **Öffentlicher Schlüssel –** geben Sie den vollständigen Pfad des öffentlichen Schlüssels an (drwcsd.pub).

Es ist nicht möglich, eine Verbindung mit dem Server ohne einen öffentlichen Schlüssel herzustellen. Der Administrator aber kann die etsprechenden Einstellungen ändern, um Verbindung ohne öffentlichen Schlüssel zuzulassen.

Wenn Sie einen nicht gültigen öffentlichen Schlüssel nutzen wollen, markieren Sie das entsprechende

Kontrollkästchen.

Beim Klicken auf **Zusätzlich** erhalten Sie Zugriff auf zusätzliche Einstellungen.

- **Stations-ID –** geben Sie die ID von **Dr.Web**, die Ihrem Computer zur Registrierung auf dem Server zugeordnet wurde.
- **Passwort –** geben Sie das Passwort von **Dr.Web** für die Verbindung zum Server.

Wenn der Modus **Verbinden als: Anfänger** gewählt ist, können Sie eine neue Registrierung auf dem zentral verwalteten Virenschutz-Server anfordern bzw. die Verbindung zu einem anderen Server konfigurieren, indem Sie die Verbindungsparameter zum Server (**Adresse**, **Port** und **Öffentlicher Schlüssel**) ändern. Nachdem die Registrierung auf dem zentral verwalteten Virenschutz-Server bestätigt wird, erhält **Dr.Web** die vom Administrator festgelegten Einstellungen.

Um das Fenster **Server-Einstellungen** zu schließen und die Änderungen zu übernehmen, klicken Sie auf **OK.** Um das Fenster zu schließen, ohne dass die Änderungen übernommen werden, klicken Sie auf **Abbrechen**.

In der Gruppe **Zusätzlich** können Sie folgende Optionen wählen:

- **Aufgaben vom Server erhalten –** um Aufgaben vom Administrator regelmäßig zu erhalten.
- **Updates vom Server erhalten –** um regelmäßige Updates für Komponenten von **Dr.Web** und Virendatenbanken vom zentral verwalteten Virenschutz-Server zu erhalten. Die Aktualisierung erfolgt gemäß den auf dem Server festgelegten Einstellungen.
- **Systemzeit mit Serverzeit synchronisieren –** um die Systemzeit auf Ihrem PC mit der Zeit auf dem zentral verwalteten Virenschutz-Server zu synchronisieren. In diesem Modus passt **Dr.Web** die Systemzeit auf Ihrem Computer regelmäßig mit der Serverzeit an.
- **Ereignisse speichern –** um Daten über aufgetretene Ereignisse für deren weiteren Versand an den zentral verwalteten Virenschutz-Server zu sammeln. Dabei werden die Informationen übermittelt, sofern eine Verbindung zum Server aufgebaut wird. Wenn das Kontrollkästchen nicht aktiviert ist, und keine Verbindung zum Server besteht, werden wichtige Informationen (z. B. zu erkannten Bedrohungen und Statistiken) verloren.
- **Mobilmodus nutzen, wenn keine Verbindung zum Server besteht –** um Updates für Virendatenbanken rechtzeitig zu erhalten.

Wenn Ihr Computer längere Zeit keine Verbindung zum zentral verwalteten Virenschutz-Server hat, wird es empfohlen, den Mobilmodus von **Dr.Web** zu aktivieren, um Updates von den Servern von **Doctor Web** rechtzeitig zu erhalten. Dafür aktivieren Sie das Kontrollkästchen **Mobilmodus nutzen, wenn keine Verbindung zum Server besteht**.

Das Kontrollkästchen **Mobilmodus nutzen, wenn keine Verbindung zum Server besteht** ist nur dann zugänglich, wenn der Betrieb von **Doctor Web** Servern im Mobilmodus auf dem zentral verwalteten Virenschutz-Server erlaubt ist.

Im Mobilmodus versucht **Dr.Web** eine Verbindung zum zentral verwalteten Virenschutz-Server aufzubauen. Es werden dabei drei Verbindungsversuche gemacht. Wenn die Verbindung fehlgeschlagen ist, wird das HTTP-Update von den Servern von **Doctor Web** durchgeführt. Die Versuche, den Server zu finden, erfolgen dauernd in den Abständen von ca. eine Minute.

Um die Einstellungen für den Mobilmodus festzulegen, klicken Sie auf **Konfigurieren.** Es öffnet sich das Fenster **Mobilmodus**.

In der Dropdown-Liste **Aktualisierungsintervalle** können Sie die Abstände festlegen, in denen die Überprüfung nach Updates auf den Servern von **Doctor Web** durchgeführt wird.

Wenn die Option **Manuell** in der Liste **Aktualisierungsintervalle** gewählt ist, wird keine Aktualisierung durchgeführt.

Wird ein Proxy-Server verwendet, markieren Sie das entsprechende Kontrollkästchen. In diesem Fall werden folgende Felder aktiv:

Einstellung	Beschreibung
Adresse	Geben Sie die Adresse des Proxy-Servers ein.
Port	Geben Sie den Port des Proxy-Servers ein.
Benutzer	Geben Sie den Kontonamen für die Verbindung zum Proxy-Server ein.
Passwort	Geben Sie das Kontopasswort ein, das für die Herstellung der Verbindung zum Proxy-Server verwendet wird.
Typ der Autorisierung	Wählen Sie den Autorisierungstyp aus, der für den Aufbau der Verbindung zum Proxy-Server benötigt wird.

Nachdem Sie die Bearbeitung abgeschlossen haben, klicken Sie auf **OK,** um die vorgenommenen Änderungen zu speichern bzw. auf **Abbrechen,** um die Änderungen zu verwerfen. Um die Verbindungseinstellungen zum Proxy-Server zu ändern, klicken Sie auf **Ändern**.

Im Mobilmodus werden nur Antivirendatenbanken aktualisiert.

Wenn Sie das Kontrollkästchen **Mobilmodus nutzen, wenn keine Verbindung zum Server besteht** deaktivieren, bevor eine Verbindung mit dem Zentralschutz-Server wieder hergestellt wird, können Antivirendatenbanken nicht mehr aktualisiert werden. Die Suche nach dem Server wird aber fortgesetzt.

Alle Änderungen, die auf dem Server für eine solche Station festgelegt werden, werden übernommen, sobald die Kommunikation zwischen **Dr.Web** und dem Server hergestellt wird.

9. Office Control

Mit **Office Control** können Sie den Zugriff auf bestimmte Webseiten, Dateien und Ordner einschränken und die im Internet oder am Rechner verbrachte Zeit kontrollieren.

Die Einschränkung des Zugriffs auf die Ressourcen des lokalen Dateisystems ermöglicht es, die Integrität und Vertraulichkeit von wichtigen Dateien aufzubewahren und diese vor der Vireninfizierung zu schützen. Es besteht die Möglichkeit, sowohl einzelne Dateien als auch komplette Verzeichnisse sowohl auf lokalen Festplatten als auch auf den externen Datenträgern zu schützen.

Das Steuern des Zugriffs auf die Webinhalte ermöglicht dem Benutzer sowohl den Schutz vor den Aufrufen unerwünschter Webseiten (Seiten, die sich dem Gewalt, Glücksspielen, etc. widmen) als auch einen kontrollierten Zugriff auf die durch die Einstellungen von **Office Control** definierten Webseiten.

9.1. Office Control konfigurieren

Die Einstellungen der Komponente können geändert werden, wenn es vom Administrator des zentral verwalteten Virenschutz-Servers, zu dem **Dr.Web** eine Verbindung herstellt, erlaubt ist.

Für den Zugriff auf die Einstellungen des Moduls **Office Control** wird das Passwort abgefragt, falls Sie das Kontrollkästchen **Dr.Web Einstellungen mit Passwort schützen** im Abschnitt Einstellungenaktiviert haben.

Office Control konfigurieren

Die Einstellungen von **Office Control** gelten für alle Benutzer des Rechners, auf dem **Dr.Web Agent** installiert ist. Im Hauptfenster werden die festgelegten Einstellungen angezeigt. Alle Benutzer können standardmäßig auf Internetressourcen oder lokale Ressourcen uneingeschränkt zugreifen. Die Zeitbeschränkung ist dabei auch deaktiviert.

Sie können die Anzeige von Benachrichtigungen über Aktionen von **Office Control** einstellen.

Internet

Standardmäßig ist für alle Benutzer der Modus **Ohne Einschränkungen** voreingestellt. Um die Einstellungen zu ändern, wählen Sie in der Dropdown-Liste einen anderen Modus aus.

Anhand der Kategorien blockieren

In diesem Modus können Sie die Kategorien der Inhalte definieren, zu denen Sie den Zugang beschränken wollen. Ebenfalls können Sie in diesem Modus selbstständig die Websites angeben, zu denen der Zugang unabhängig von anderen Beschränkungen verboten oder erlaubt wird.

Alles blockieren, ausschließlich der Webseiten auf der Whitelist

In diesem Modus wird der Zugriff auf alle Webressource gesperrt, die in der Whitelist nicht aufgeführt sind.

Sichere Suche

In jedem Modus außer **Ohne Einschränkungen** können Sie die Option **Sichere Suche** aktivieren. Bei dieser Funktion handelt es sich darum, dass bestimmte unerwünschte Webressourcen in Suchergebnissen automatisch ausgeblendet werden.

Zeit

In diesem Abschnitt werden die Einschränkungen für die Arbeitszeit am Computer und im Internet festgelegt.

Standardmäßig wird die Arbeit am Computer und im Internet für alle Benutzer zeitlich nicht eingeschränkt.

Zugriff zeitlich einschränken

1. Wählen Sie die Uhrzeit und die Wochentage, an welchen der Zugang zu dem Internet einem Benutzer verweigert werden soll, und markieren Sie die entsprechenden Zeitfenster blau.
   - um ein Zeitfenster zu markieren, klicken Sie einmal darauf mit der linken Maustaste;
   - um mehrere nebeneinander stehende Zeitfenster gleichzeitig zu markieren, klicken Sie einmal mit der linken Maustaste auf das erste Zeitfenster, halten Sie die linke Maustaste gedrückt und markieren Sie das ganze notwendige Zeitfenster.
2. Wählen Sie die Uhrzeit und die Wochentage, an welchen der Zugang zu dem Computer einem Benutzer verweigert werden soll, und markieren Sie die entsprechenden Zeitfenster rot.
   - um ein Zeitfenster zu markieren, klicken doppelt darauf mit der linken Maustaste;
   - um mehrere nebeneinander stehende Zeitfenster gleichzeitig zu markieren, klicken Sie doppelt mit der linken Maustaste auf das erste Zeitfenster, halten Sie die linke Maustaste gedrückt und markieren Sie das ganze notwendige Zeitfenster.

Wenn die Einschränkung der Computer- bzw. Internetnutzung eingeschaltet ist, wird die Option **Ändern des Systemdatums bzw. der Systemzeit verbieten** im Bereich Selbstschutz in den Grundeinstellungen aktiviert.

Verzeichnisse und Dateien

Standardmäßig kann ohne Einschränkungen auf Dateien und Verzeichnisse zugegriffen werden. Aktivieren Sie diese Option und fügen Sie Objekte hinzu, auf die nicht zugegriffen werden darf.

Beachten Sie, dass bei dieser Zugriffseinschränkung nicht garantiert werden kann, dass auf die hinzugefügten Objekte von externen Quellen oder anderen Betriebssystemen aus, die auf dem Rechner installiert sind, nicht zugegriffen werden kann.

10. Ausnahmen

Um auf bestimmte Webseiten, Dateien und Ordner zugreifen sowie Prozesse vom Scan durch Schutzmodule ausschließen zu können, fügen Sie die gewünschten Objekte der Ausnahmeliste hinzu. Beachten Sie aber dabei: Der Administrator Ihres Antivirus-Netzweks kann Ihnen jegliche Änderungen in diesem Abschnitt verweigern.

10.1. Webseiten

Wenn Sie die von **Doctor Web** nicht empfohlenen Webseiten trotzdem besuchen wollen, fügen Sie diese zu Ausnahmen hinzu. Danach können Sie auf diese Webseiten zugreifen. Die Webseiten werden dabei trotzdem gescannt. Standardmäßig ist die Liste leer. Falls eine Webadresse zur Whitelist hinzugefügt wird, wird der Zugriff darauf unabhängig von anderen Einstellungen von **SpIDer Gate** zugelssen. Beachten Sie: Wenn eine Webseite gleichzeitig zur Blacklist von **Office Control** und zur Ausnahmeliste hinzugefügt ist, können Sie auf sie nicht zugreifen.

Liste von Domainadressen erstellen

1. Ins Eingabefeld tragen Sie den Domainnamen oder einen Teil des Domainnamens der Website ein, zu welcher Sie den Zugang unabhängig von anderen Beschränkungen erlauben wollen.
   - um eine bestimmte Website zur Liste zuzufügen, tragen Sie ihre Adresse ein (z.B. `www.example.com`). Der Zugang zu allen auf dieser Website untergebrachten Inhalten wird erlaubt;
   - um den Zugang zu den Websites zu erlauben, deren Adressen einen bestimmten Text enthalten, tragen Sie diesen Text ins Feld ein. Zum Beispiel: Wenn Sie den Text `example`, eintragen, wird der Zugang zu Adressen **example**.com, **example**.test.com, test.com/**example**, test.**example**222.de usw. erlaubt;
   - um den Zugang zu einer bestimmten Domain zu erlauben, geben Sie den Domainnamen mit dem Zeichen„.“ an. In diesem Fall wird der Zugang zu allen sich auf dieser Domain befindenden Inhalten erlaubt. Wenn das Zeichen „/“ bei der Angabe von Domain verwendet wird, dann gilt der Teil vom Zeichen „/“ links als Domainname und von diesem Zeichen rechts als Teil der auf dieser Domain erlaubten Adresse. Zum Beispiel: Wenn Sie den Text`example.com/test` eintragen, werden alle Adressen wie **xample.com/test**11, template.**example.com/test**22 usw. erlaubt.

   Die eingegebene Zeile kann beim Einfügen in die Liste in eine universelle Zeile konvertiert werden.

2. Klicken Sie auf . Die angegebene Adresse wird in die Liste aufgenommen.
3. Bei Bedarf wiederholen Sie die Schritte 1 und 2, um andere Adressen hinzuzufügen. Um eine Adresse aus der Whitelist zu entfernen, wählen Sie das entsprechende Element in der Liste aus und klicken Sie auf .

10.2. Dateien und Verzeichnisse schützen

In diesem Abschnitt wird die Liste der von der Prüfung durch **SpIDer Guard** ausgenommenen Verzeichnisse und Dateien konfiguriert. Zu solchen können Quarantäne-Ordner, Arbeitsordner einiger Programme, temporäre Dateien (Auslagerungsdateien) u. ä. gezählt werden.

Standardmäßig ist die Liste leer. Fügen Sie zur Ausnahmeliste bestimmte Ordner und Dateien hinzu oder verwenden Sie Masken, um bestimmte Dateigruppen nicht scannen zu lassen.

Ausnahmeliste erstellen

Um ein Verzeichnis oder eine Datei zur Ausnahmeliste hinzuzufügen, führen Sie eine der folgenden Aktionen durch:

- um ein bestimmtes existierendes Verzeichnis oder eine Datei anzugeben, klicken Sie auf . In geöffneten Fenster klicken Sie auf **Durchsuchen** und wählen Sie ein Verzeichnis oder eine Datei aus. Sie können den kompletten Pfad des Verzeichnisses oder der Datei manuell im Eingabefeld angeben sowie den Eintrag im Eingabefeld vor dem Hinzufügen zu der Liste bearbeiten;
- um alle Dateien oder Verzeichnisse mit einem bestimmten Namen von der Prüfung auszunehmen, geben Sie diesen Namen in das Eingabefeld ein. Die Angabe des Pfades der Datei oder des Verzeichnisses ist in diesem Fall nicht erforderlich;
- um die Dateien oder Verzeichnisse einer bestimmten Art von der Prüfung auszunehmen, geben Sie in das Eingabefeld eine Maske ein, die diese Objekte definiert.
- klicken Sie auf **OK**. Die gewählte Datei erscheint in der Liste.
- bei Bedarf wiederholen Sie die Schritte 1 und 2, um andere Dateien oder Verzeichnisse hinzuzufügen. Um eine Datei oder ein Verzeichnis aus der Liste der Ausnahmen zu entfernen, wählen Sie das entsprechende Element in der Liste aus und klicken Sie auf .

- `C:\folder` oder `C:\folder\**` – nimmt alle Dateien im Verzeichnis C:\folder von der Prüfung aus. Die Dateien in Unterverzeichnissen werden überprüft.
- `C:\folder\*` – nimmt alle Dateien im Verzeichnis C:\folder sowie in allen Unterverzeichnissen auf beliebiger Ebene von der Prüfung aus.
- `C:\folder\*.txt` – nimmt die *.txt Dateien im Verzeichnis C:\folder von der Prüfung aus. In den Unterverzeichnissen werden die *.txt Dateien überprüft.
- `C:\folder\*\*.txt` – schließt die Prüfung von *.txt Dateien nur in Unterverzeichnissen auf der ersten Ebene des Verzeichnisses C:\folder aus.
- `C:\folder\**\*.txt` – schließt die Prüfung von *.txt Dateien in Unterverzeichnissen auf beliebiger Ebene des Verzeichnisses C:\folder aus. In dem Verzeichnis C:\folder selbst werden aber die *.txt Dateien überprüft.

10.3. Programme und Prozesse

In dieser Rubrik werden Programme und Prozesse angegeben, die aus der Prüfung durch **SpIDer Guard**, **SpIDer Gate** und **SpIDer Mail** ausgeschlossen werden sollen.

Ausnahmeliste erstellen

1. Um ein Programm oder einen Prozess zur Ausnahmeliste hinzuzufügen, klicken Sie auf . Im geöffneten Fenster klicken die Schaltfläche **Durchsuchen** an und wählen Sie im nächsten geöffneten Fenster eine Datei aus.
2. Im Einstellungsfenster geben Sie an, von welchen Modulen die gewählte Datei nicht überprüft werden soll.
3. Klicken Sie auf **OK**. Das gewählte Objekt wird in der Ausnahmeliste angezeigt.
4. Wiederholen Sie bei Bedarf diese Schritte, um andere Programme und Dateien zur Ausnahmeliste hinzuzufügen.
5. Um eine Datei aus der Liste zu entfernen, wählen Sie in der Liste die gewünschte Datei aus und klicken Sie auf .

10.4. Antispam

In diesem Fenster werden Listen der Absender erstellt, deren E-Mails vom E-Mail-Wächter **SpIDer Mail** ignoriert bzw. ohne Analyse als Spam angesehen werden.

Wenn die Absenderadresse zur Whitelist hinzugefügt wird, wird die E-Mail auf Spam nicht geprüft. Wenn die Absenderadresse zur Blacklist hinzugefügt wird, wird die E-Mail ohne zusätzliche Analyse als Spam eingestuft. Per Default sind beide Listen leer.

Antispam-Listen erstellen

1. Geben Sie in das Eingabefeld die E-Mail-Adresse des Absenders bzw. die Maske für E-Mail-Adressen der Absender ein, deren E-Mails von Ihnen ohne Analyse automatisch bearbeitet werden sollen. Eingabemethoden:
   - um einen bestimmten Absender zur Liste hinzuzufügen, geben Sie seine komplette E-Mail-Adresse (z.B. `name@beispielweb.de`) an. Alle E-Mails, die von dieser Adresse erhalten werden, werden ohne Analyse bearbeitet;
   - um die Absender, die ähnliche E-Mail-Adressen benutzen, zur Liste hinzuzufügen, verwenden Sie die Zeichen „`*`" und „`?`" zum Ersetzen von dem abweichenden Teil der E-Mail-Adresse. Dabei ersetzt das Zeichen „`*`" eine beliebige Reihenfolge von Zeichen und das Zeichen „`?`" – ein (beliebiges) Zeichen. Zum Beispiel: wenn Sie die Adresse `name*@beispielweb.de`, eintragen, dann werden die E-Mails von den Absendern mit den Adressen **name@beispielweb.de, name**1**@beispielweb.de, name**_moj**@beispielweb.de** usw. werden ohne Analyse bearbeitet;
   - um E-Mails von E-Mail-Adressen einer bestimmten Domain garantiert zu erhalten, benutzen Sie das „`*`" Symbol anstatt des Benutzernamens. Beispiel: um alle E-Mails z.B. von Adressaten auf der Domain beispielweb.de zu erhalten, geben Sie `*@beispielweb.de` ein.
2. Um die eingegebene E-Mail-Adresse zur Liste hinzuzufügen, klicken Sie auf .
3. Gegebenenfalls können Sie die Schritte 1 und 2 wiederholen, um weitere Adressen hinzuzufügen. Um einen Adressaten aus der Liste zu entfernen, wählen Sie das entsprechende Element in der Liste aus und klicken Sie auf .

11. Schutzkomponente

11.1. SpIDer Guard

SpIDer Guard ist ein speicherresidenter Antivirus-Wächter, der Dateien und laufende Prozesse in Echtzeit scannt und das System vor verdächtigen und bösartigen Aktivitäten schützt.

Auf der Festplatte prüft dieser Echtzeit-Scanner standardmäßig nur erstellte und geänderte Dateien. Auf Wechseldatenträgern prüft er hingegen alle geöffneten Dateien. Diese Komponente dient auch zur permanenten Überwachung von Programmaktionen und Sperrung von verdächtigen Aktivitäten. Infizierte Objekte, die durch **SpIDer Guard** erkannt wurden, werden entsprechend behandelt.

Sollte eine Datei im Archiv oder E-Mail-Anhang infiziert sein, wird das Schadobjekt durch den Wächter beim Extrahieren erkannt, bevor der Rechner infiziert werden kann. Um das Eindringen schädlicher Objekte auf Ihren Rechner zu verhindern, verwenden Sie den **SpIDer Mail** E-Mail-Wächter.

Bei Entdeckung infizierter Objekte nimmt **SpIDer Guard** Aktionen vor, die den vordefinierten Einstellungen entsprechen. Durch die entsprechende Veränderung von Einstellungen können Sie die automatische Reaktion des Wächters auf Virenereignisse bestimmen.

Dr.Web kann unter Umständen mit MS Exchange Server inkompatibel sein. Falls Probleme damit entstehen, fügen Sie die Datenbanken sowie das Transaktionsprotokoll von MS Exchange Server zur Ausnahmeliste von **SpIDer Guard** hinzu.

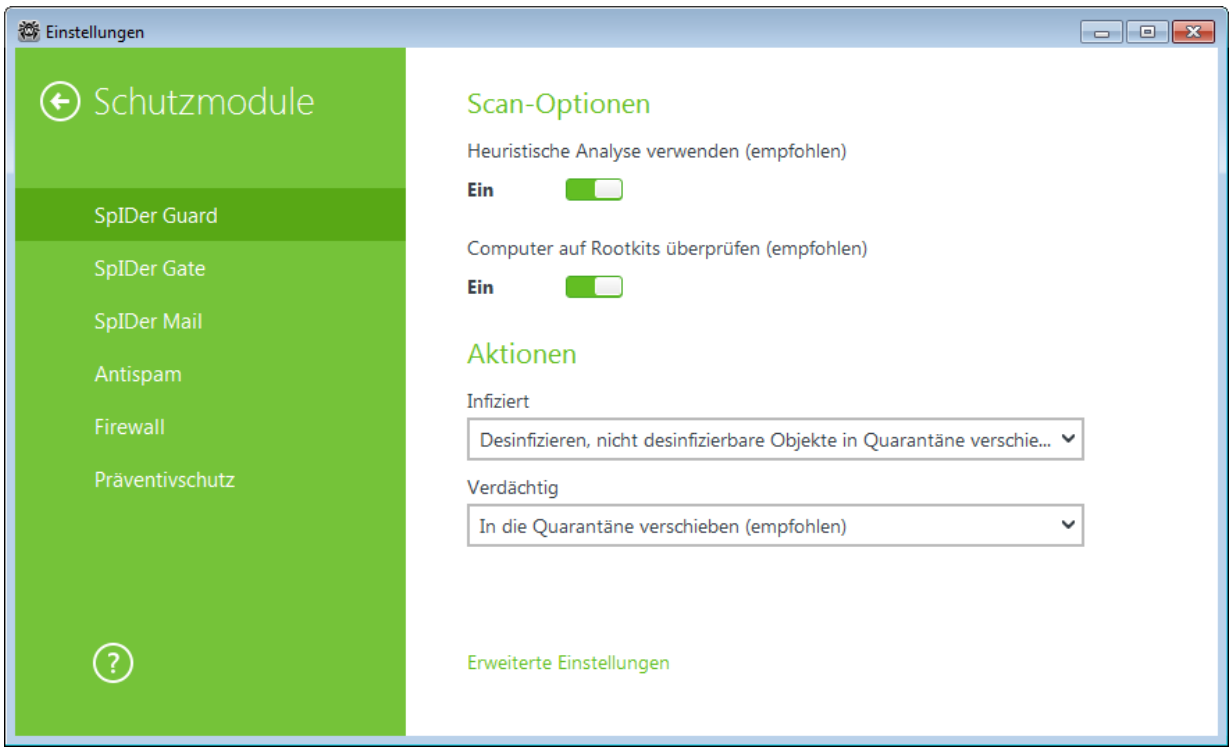
Standardmäßig startet **SpIDer Guard** automatisch beim Start des Betriebssystems. Der einmal gestartete **SpIDer Guard** kann während der laufenden Sitzung des Betriebssystems nicht deaktiviert werden.

11.1.1. SpIDer Guard konfigurieren

Die Einstellungen der Komponente können geändert werden, wenn es vom Administrator des zentral verwalteten Virenschutz-Servers, zu dem **Dr.Web** eine Verbindung herstellt, erlaubt ist.

Um **SpIDer Guard** einstellen zu können, müssen Sie ein entsprechendes Passwort eingeben, wenn im Bereich Einstellungen die Option **Dr.Web Einstellungen mit Passwort schützen** aktiviert ist.

Die standardmäßigen Einstellungen sind optimal für die meisten Fälle. Ändern Sie diese nur bei Bedarf.



Scan-Optionen

Heuristische Analyse

Standardmäßig verwendet **SpIDer Guard** beim Scannen die heuristische Analyse. Wenn diese Option deaktiviert ist, verwendet der Scanner nur vorhandene Signaturen bekannter Viren.

Hintergrundüberprüfung auf Infizierung

Die Komponente von **Dr.Web Anti-Rootkit** erlaubt es, Ihr Betriebssystem auf komplizierte Bedrohungen im Hintergrundmodus zu überprüfen und führt bei Bedarf die Desinfizierung der aktiven Infektion durch.

Wenn diese Option aktiviert ist, bleibt **Dr.Web Anti-Rootkit** permanent im Arbeitsspeicher. Im Gegensatz zu der Dateiüberprüfung durch **SpIDer Guard** erfolgt die Suche nach den Rootkits im BIOS des Computers und in kritischen Windows-Bereichen wie etwa in Autostart-Objekten, gestarteten Prozessen und Modulen, MBR/VBR-Laufwerken, dem Arbeitsspeicher u. a.

Eines der Schlüsselkriterien bei Funktion von **Dr.Web-Anti-Rootkit** ist der schonende Verbrauch von Ressourcen des Betriebssystems (Prozessorzeit, RAM u. s. w.) sowie die Berücksichtigung der Leistungsfähigkeit der Hardware.

Bei der Erkennung von Bedrohungen informiert **Dr.Web Anti-Rootkit** Sie darüber und neutralisiert die gefährlichen Einwirkungen.

Bei der Durchführung der Hintergrundüberprüfung auf Rootkits werden Dateien und Ordner von der Überprüfung ausgeschlossen, die auf der ensprechenden Registerkarte eingegeben sind.

Um die Überprüfung im Hintergrundmodus zu aktivieren, aktivieren Sie die Option **Computer auf Rootkits überprüfen (empfohlen).**

Die Hintergrundüberprüfung wird durch das Deaktivieren des **SpIDer Guard** Wächters nicht betroffen. Wenn die Einstellung aktiviert ist, erfolgt die Überprüfung im Hintergrundmodus unabhängig davon, ob **SpIDer Guard** aktiviert bzw. deaktiviert ist.

Aktionen

In diesem Abschnitt wird die Reaktion des **SpIDer Guard** Wächters bei der Erkennung infizierter oder verdächtiger Dateien sowie schädlicher Programme konfiguriert.

Die Reaktionen werden für jede Kategorie von Objekten separat konfiguriert:

- **Infizierte Objekte,** die mit bekannten und (vermutlich) desinfizierbaren Viren infiziert sind.
- **Verdächtige Objekte,** vermutlich von Viren infiziert oder schädliche Objekte enthalten.
- Verschiedene potentiell gefährliche Objekte.

Sie haben die Möglichkeit, die Reaktionen des **SpIDer Guard** Wächters auf die Entdeckung jedes Typs der obengenannten Objekte separat zu verändern. Dabei hängen die zugänglichen Reaktionen vom Typ des Virenereignisses ab.

Im Standardmodus versucht der **SpIDer Guard** Wächter die mit bekannten und potentiell desinfizierbaren Viren infizierten Dateien zu desinfizieren. Die übrigen höchstgefährlichen Objekte werden in die Quarantäne verschoben. Scherzprogramme, Hacktools und unzuverlässige Objekte werden im Standardmodus *ignoriert.* Die Reaktionen des **SpIDer Guard** Wächters sind den entsprechenden Reaktionen des **Dr.Web Scanners** ähnlich.

Es bestehen folgende Reaktionen auf die entdeckten Objekte:

Aktion	Beschreibung
Desinfizieren, in Quarantäne verschieben	Den Zustand des Objektes vor seiner Infizierung wiederherstellen. Wenn das Virus nicht desinfizierbar ist oder der Versuch der Desinfizierung nicht erfolgreich war, wird das Objekt in die Quarantäne verschoben. Diese Aktion ist nur für die mit bekannten desinfizierbaren Viren infizierten Objekte möglich. Ausgenommen sind Trojaner und infizierte Dateien innerhalb der zusammengesetzten Objekte.
Desinfizieren, nicht desinfizierbare Objekte löschen	Den Zustand des Objektes vor seiner Infizierung wiederherstellen. Wenn das Virus nicht desinfizierbar ist oder der Versuch der Desinfizierung nicht erfolgreich war, wird das Objekt gelöscht. Diese Aktion ist nur für die mit bekannten desinfizierbaren Viren infizierten Objekte möglich. Ausgenommen sind Trojaner und infizierte Dateien innerhalb der zusammengesetzten Objekte.
Löschen	Das Objekt entfernen. Für die Bootsektoren werden keine Aktionen durchgeführt.
In Quarantäne verschieben	Das Objekt in das spezielle Verzeichnis der Quarantäne verschieben. Für die Bootsektoren werden keine Aktionen durchgeführt.
Überspringen	Das Objekt ohne Anwendung jeglicher Aktionen und ohne Benachrichtigung überspringen. Diese Aktion ist nur für schädliche Programme möglich: Adware, Dialer, Scherzprogramme, Riskware und Hacktools.
Informieren	Eine Benachrichtigung anzeigen und das Objekt ohne Anwendung jeglicher Aktionen überspringen. Diese Aktion ist nur für verdächtige Objekte und Schadprogramme möglich.

Der **SpIDer Guard** Wächter durchsucht keine zusammengesetzten Objekte, deswegen werden keine Aktionen für diese Objekte bzw. für die darin enthaltenen Dateien durchgeführt.

Die Backup-Kopien der bearbeiteten Objekte werden in der Quarantäne gespeichert.

Virenprüfung

In dieser Gruppe der Einstellungen wird es vorgegeben, bei welchen Aktionen mit dem Objekt seine Prüfung durch den **SpIDer Guard** Wächter durchgeführt werden soll.

Einstellung	Beschreibung
Optimal (empfohlen)	Der Standardwert. In diesem Modus wird das Scannen nur in den folgenden Fällen durchgeführt: • für die Objekte auf Festplatten – beim Starten oder Erstellen von Dateien, sowie bei den Versuchen, in die vorhandenen Dateien oder Bootsektoren zu schreiben; • für die Objekte auf Wechselmedien – bei jedem Zugriff auf Dateien oder Bootsektoren (Lesen, Schreiben, Ausführen).
Vergesslich	In diesem Modus wird das Scannen aller Dateien und Bootsektoren bei jedem Zugriff (Erstellen, Lesen, Schreiben, Ausführen) auf Festplatten, Netzwerklaufwerken sowie Wechselmedien durchgeführt.

Im optimalen Modus wird die Ausführung der EICAR-Testdatei von **SpIDer Guard** nicht unterbrochen und diese Aktion nicht als gefährlich definiert, da diese Datei keine Bedrohung für den Computer darstellt. Allerdings wird sie beim Kopieren und Erstellen auf dem Computer automatisch von **SpIDer Guard** wie ein schädliches Programm bearbeitet und standardmäßig in die **Quarantäne** verschoben.

Es wird empfohlen, den Modus **Optimal** nur nach der Prüfung aller Festplatten unter Anwendung von **Dr.Web Scanner** zu nutzen. Dabei wird das Eindringen neuer Viren und anderer bösartiger Programme auf den PC über die Wechselmedien verhindert. Es wird jedoch hierbei keine wiederholte Prüfung bereits geprüfter Objekte durchgeführt.

Der Modus **Paranoid** sorgt für das maximale Sicherheitsniveau, vergrößert jedoch dabei die Belastung am PC.

Die Prüfung von Objekten auf Netzwerklaufwerken und Wechselmedien wird in jedem Modus nur beim Setzen entsprechender Häkchen in der Einstellungsgruppe **Zusätzliche Aufgaben** durchgeführt.

Manche Wechselmedien (insbesondere externe Festplatten mit USB-Schnittstelle) können im Betriebssystem als Festplatten dargestellt werden. Deswegen sollen solche Geräte unter besonderer Vorsicht genutzt und beim Anschließen an PC auf Viren unter Anwendung von **Dr.Web Scanner** geprüft werden.

Die Dateien innerhalb von Archiven und E-Mail-Fächern werden im Standardmodus nicht geprüft. Verzicht auf die Prüfung der Archive und E-Mail-Fächer beim ununterbrochenen Lauf des **SpIDer Guard** Wächters führt nicht zum Eindringen von Viren auf PC, sondern schiebt lediglich das Moment deren Entdeckung hinaus. Beim Entpacken eines infizierten Archivs oder beim Öffnen einer infizierten E-Mail wird es vom Betriebssystem versucht, das infizierte Objekt auf die Festplatte zu schreiben. Dabei aber wird das schädliche Objekt unvermeidlich vom **SpIDer Guard** Wächter entdeckt.

Zusätzliche Aufgaben

Diese Gruppe der Einstellungen ermöglicht es, Scaneinstellungen in Echtzeit zu konfigurieren. Diese Konfiguration wird unabhängig von dem ausgewählten Modus des **SpIDer Guard** Wächters angewendet.

Hier können Sie die Virenprüfung wie folgt konfigurieren:

- für Dateien gestarteter Prozesse unabhängig von ihrem Speicherort (diese Option ist standardmäßig aktiviert);
- für Installationsdateien;
- für Dateien auf Netzwerklaufwerken;
- für Dateien und Bootsektoren auf Wechselmedien (diese Option ist standardmäßig aktiviert).

SpIDer Guard blockiert standardmäßig den automatischen Start der aktiven Inhalte von externen Datenträgern (CDs/DVDs, Flash-Speichern usw.). Diese Funktion verhindert die eventuelle Infizierung Ihres Rechners über externe Datenträger.

Falls Probleme bei der Installation der Programme, die sich auf die Datei autorun.inf zugreifen, entstehen, ist es empfehlenswert, die Option **Autoruns von Wechseldatenträgern blockieren vorübergehend zu deaktivieren.**

11.2. SpIDer Gate

SpIDer Gate ist ein Web-Antivirus, der den eingehenden HTTP-Datenverkehr automatisch überwacht und die Übermittlung von Objekten (standardmäßig) blockiert, die bösartige Programme enthalten. Das HTTP-Protokoll verwenden Webbrowser, Download-Manager und viele andere Anwendungen, die Daten mit Webservern austauschen, d. h. die das Internet verwenden.

Standardmäßig blockiert **SpIDer Gate** alle über das Netzwerk übertragenen Objekte, die bösartige Programme enthalten.

Durch Änderung der Einstellungen von **SpIDer Gate** können Sie die Überwachung des eingehenden oder ausgehenden Datenverkehrs deaktivieren sowie eine Liste der Anwendungen erstellen, deren HTTP-Datenverkehr immer und vollständig geprüft wird. Einzelne Anwendungen können bei Bedarf von der Prüfung ausgeschlossen werden.

Bei Standardeinstellungen werden die über das Netzwerk geschickten Objekte, die Schadprogramme enthalten, von **SpIDer Gate** blockiert. Ebenso ist die URL-Filterung der nicht empfohlenen Websites sowie der Websites, die für die Virenverbreitung bekannt sind, standardmäßig aktiviert.

SpIDer Gate ist speicherresident und startet standardmäßig automatisch beim Start des Betriebssystems.

11.2.1. SpIDer Gate konfigurieren

Die Einstellungen der Komponente können geändert werden, wenn es vom Administrator des zentral verwalteten Virenschutz-Servers, zu dem **Dr.Web** eine Verbindung herstellt, erlaubt ist.

Um **SpIDer Gate** einstellen zu können, müssen Sie das entsprechende Passwort eingeben, wenn im Bereich Einstellungen die Option **Dr.Web Einstellungen mit Passwort schützen** aktiviert ist.

Die standardmäßigen Einstellungen sind optimal für die meisten Fälle. Ändern Sie diese nur bei Bedarf.

Traffic der IM-Clients überprüfen

In der Gruppe **Scan-Optionen** können Sie die Prüfung von Links und Daten aktivieren, die durch die Clients der Instant-Messaging-Systeme (Mail@RU Agent, ICQ und Jabber-Clients) übermittelt werden. Dabei wird nur der eingehende Datenverkehr übergeprüft. Standardmäßig ist diese Option aktiviert.

Die in den Nachrichten übermittelten Links werden aufgrund der Einstellungen von **SpIDer Gate** überprüft: die Links zu Websites, die als Quellen der Virenverbreitung bekannt sind, werden automatisch gesperrt. Die Links zu nicht empfohlenen Websites sowie URLs, die auf Antrag des Rechteinhabers hinzugefügt wurden, werden in dem Fall blockiert, wenn entsprechende Einstellungen in dem Bereich **Sperrparameter** aktiviert sind. Dabei wird die Whitelist der Websites und von der Prüfung ausgenommene Anwendungen berücksichtigt.

Die durch die Clients der Instant-Messaging-Systeme übermittelten Dateien werden auch überprüft. Sollte eine Bedrohung erkannt werden, wird die Übermittlung einer solchen Datei gesperrt, sofern die entsprechende Einstellung in dem Bereich **Programme sperren** aktiviert ist. Die Viren werden automatisch gesperrt, wenn die Option **Verkehr und URL bei IM-Clients überprüfen** aktiviert ist.

Sperrparameter

In der Gruppe **Sperrparameter** können Sie das automatische Sperren des Zugangs zu den URLs, die auf Antrag des Rechteinhabers hinzugefügt wurden (dafür markieren Sie das entsprechende Kontrollkästchen), sowie zu den nicht empfohlenen Websites, die als unzuverlässig bekannt sind (dafür setzen Sie ein Häkchen bei **Nicht empfohlene Websites blockieren**), einrichten. Im Abschnitt **Ausnahmen** können Sie Websites angeben, auf die der Zugriff trotz festgesetzter Einschränkungen zu erlauben ist.

Standardmäßig blockiert **SpIDer Gate** den Zugriff auf die Websites, die als Quellen der Viren- und Malware-Verbreitung bekannt sind. Dabei wird die Liste der von der Prüfung ausgenommenen Anwendungen berücksichtigt.

Programme sperren

Der HTTP-Wächter **SpIDer Gate** blockiert standardmäßig folgende bösartige Programme:

- Verdächtig;
- Riskware;
- Dialer;
- Hacktool;
- Adware;
- Scherzprogramme.

Standardmäßig werden verdächtige Programme, Adware und Dialer blockiert.

Objekte sperren

SpIDer Gate kann auch nicht geprüfte und beschädigte Objekte sperren. Standardmäßig sind diese Optionen deaktiviert.

Zusätzliche Aufgaben

Sie Können die Überprüfung der Archive und Installationspakete konfigurieren. Standardmäßig ist die Option für die Überprüfung der Archive und Installationspakete deaktiviert.

In diesem Fenster können Sie die **Scanpriorität** einstellen – Verteilung der Ressourcen je nach Scanpriorität des Traffics. Bei geringer Prüfungspriorität wird die Internetverbindung verlangsamt, weil der HTTP-Wächter **SpIDer Gate** länger auf die Datenladung warten und ein größeres Informationsvolumen prüfen muss. Beim Erhöhen der Scanpriorität wird die Prüfung öfter durchgeführt, was dem Wächter möglich macht, die Daten schneller weiterzuleiten. Somit wird die Internetverbindung schneller. Bei öfteren Prüfungen erhöht sich jedoch die Belastung des Prozessors.

Es besteht auch die Möglichkeit zur Auswahl des Typs des zu prüfenden HTTP-Traffics. Per Default wird nur der eingehende Traffic geprüft. Dabei werden die festgelegten Aktionen, die Whitelist der Websites und von der Prüfung ausgenommene Anwendungen berücksichtigt.

11.3. SpIDer Mail

SpIDer Mail ist ein E-Mail-Wächter, der Zugriffe von laufenden E-Mail-Clients auf Mailserver überwacht. Dabei wird der Datenverkehr über die Protokolle POP3/SMTP/IMAP4(IMAPv4rev1)/NNTP überprüft. Dadurch werden E-Mail-Viren erkannt und desinfiziert, bevor der E-Mail-Client infizierte E-Mails vom Server empfängt oder eine E-Mail an Server gesendet wird.

Die Standardeinstellungen des Programms sind für Anfänger optimal und sorgen für das maximale Niveau an Sicherheit bei einer minimalen Einmischung des Benutzers. Dabei werden jedoch einige Möglichkeiten der Mail-Programme blockiert (z.B.: Versand eines Briefes an mehrere Adressen kann als Massenversand eingestuft werden, oder der eingehende Spam wird nicht erkannt). Desweiteren geht die Möglichkeit verloren, nützliche Informationen aus den automatisch vernichteten E-Mails (aus dem nicht infizierten Textteil) zu erhalten. Die erfahrenen Benutzer können die Parameter der E-Mail-Prüfung

und Reaktionen auf verschiedene Ereignisse ändern.

Funktionsweise

Der E-Mail-Wächter empfängt alle eingehenden E-Mails anstatt des E-Mail-Clients und unterzieht sie einer Virenprüfung mit der maximalen Detailuntersuchung. Wenn keine Viren bzw. verdächtige Objekte erkannt werden, wird die E-Mail dem Mail-Client in einer „transparenten" Form übergeben, als ob sie direkt vom Server eingegangen wäre. Analog werden die ausgehenden E-Mails vor dem Absenden zum Server geprüft.

Die Reaktion des Programms bei der Erkennung infizierter und verdächtiger eingehender E-Mails sowie E-Mails, welche nicht geprüft werden konnten (z.B. E-Mails mit komplexer Datenstruktur), ist standardmäßig diese (mehr zu diesen Einstellungen finden Sie unter SpIDer Mail konfigurieren):

- Aus den infizierten E-Mails werden schädliche Informationen entfernt (diese Aktion wird *Desinfizieren* eines Briefes genannt), dann werden sie wie üblich zugestellt;
- E-Mails mit verdächtigen Objekten werden als separate Dateien in die Quarantäne verschoben, dem E-Mail-Programm wird eine Benachrichtigung darüber zugesandt (diese Aktion wird *Verschieben* eines Briefes genannt). Die verschobenen E-Mails werden vom POP3- oder IMAP4-Server entfernt;
- Nicht infizierte E-Mails und die E-Mails, die keine Prüfung bestanden haben, werden ohne Änderungen übergeben (*durchgelassen*).

Infizierte oder verdächtige ausgehende E-Mails werden nicht an Server weitergegeben. Der Benutzer wird in diesem Fall darüber benachrichtigt (die E-Mail wird dabei vom E-Mail-Client gespeichert).

Dr.Web Scanner kann ebenfalls Viren in den Postfächern mancher Formate entdecken, der E-Mail-Wächter **SpIDer Mail** hat jedoch vor dem **Scanner** einige Vorteile:

- Nicht alle Formate von Postfächern populärer Programme werden vom**Scanner** unterstützt; bei der Verwendung des E-Mail-Wächters landen infizierte E-Mails erst gar nicht in dem Postfach;
- **Scanner** prüft die Postfächer nur auf Anfrage des Benutzers und nicht beim Empfang der E-Mails. Dieser Vorgang kann außerdem den Rechner stark belasten und einige Zeit dauern.

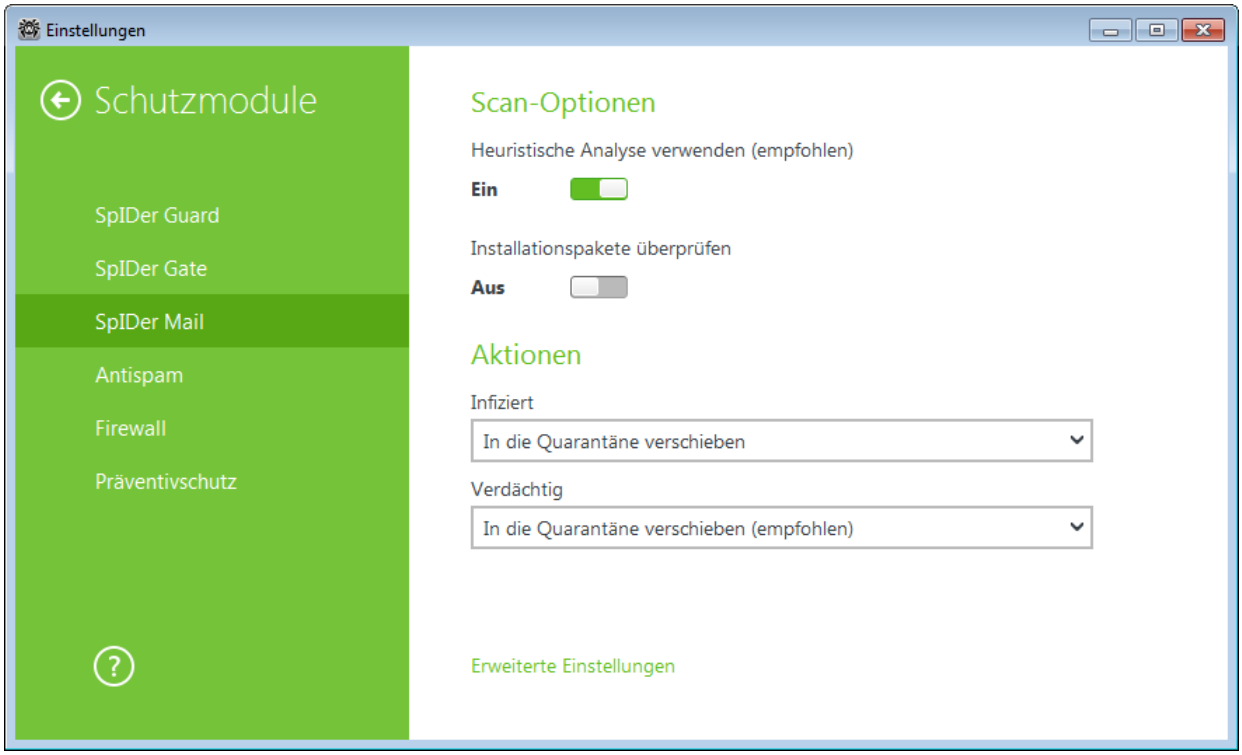
Wenn alle Komponenten die Standardeinstellungen verwenden, erkennt **SpIDer Mail** als erster Viren und verdächtige Objekte, die sich über E-Mails verbreiten. Er erfordert also sehr wenig CPU-Ressourcen. Die anderen Komponenten brauchen für die Prüfung der E-Mail-Dateien in diesem Fall nicht verwendet zu werden.

11.3.1. SpIDer Mail konfigurieren

Die Einstellungen der Komponente können geändert werden, wenn es vom Administrator des zentral verwalteten Virenschutz-Servers, zu dem **Dr.Web** eine Verbindung herstellt, erlaubt ist.

Um **SpIDer Mail** einstellen zu können, müssen Sie ein entsprechendes Passwort eingeben, wenn im Bereich Einstellungen die Option **Dr.Web Einstellungen mit Passwort schützen** aktiviert ist

Die standardmäßigen Einstellungen sind optimal für die meisten Fälle. Ändern Sie diese nur bei Bedarf.



Scanoptionen

Mit dieser Gruppe der Einstellungen werden die erweiterten Parameter zur Überprüfung von E-Mails konfiguriert:

- Nutzung der heuristischen Analyse – in diesem Modus werden spezielle Mechanismen verwendet, die es erlauben, die verdächtigen Objekte, die mit großer Wahrscheinlichkeit mit noch unbekannten Viren infiziert sind, in E-Mails zu entdecken. Um die heuristische Analyse zu deaktivieren, wählen sie das Häkchen bei **Heuristischer Analyse (empfohlen)** ab;
- Prüfung der Installationspakete. Standardmäßig ist diese Option deaktiviert.

Aktionen

Im Standardmodus versucht der Wächter **SpIDer Mail** die mit bekannten und potentiell desinfizierbaren Viren infizierten E-Mails wiederherzustellen. Die nicht desinfizierbaren und verdächtigen E-Mails sowie Adware und Dialer werden in die Quarantäne verschoben. Die übrigen E-Mails werden vom E-Mail-Wächter ohne Änderungen weitergegeben (*durchgelassen*).

Die Reaktionen des Wächters **SpIDer Mail** sind analog den entsprechenden Reaktionen des **Dr.Web Scanners**.

Sie können dem E-Mail-Wächter **SpIDer Mail** die folgenden Reaktionen vorschreiben:

Aktion	Beschreibung
Desinfizieren, in Quarantäne verschieben	Den Zustand der E-Mail vor seiner Infizierung wiederherstellen. Wenn das Virus nicht desinfizierbar ist oder der Versuch der Desinfizierung nicht erfolgreich war, wird das Objekt in die Quarantäne verschoben. Diese Aktion ist nur für die mit bekannten desinfizierbaren Viren infizierten E-Mails möglich. Ausgenommen sind Trojaner, die bei Entdeckung gelöscht werden. Die Wiederherstellung von Dateien innerhalb von Archiven ist nicht möglich, unabhängig vom Virustyp.

Aktion	Beschreibung
Desinfizieren, nicht desinfizierbare Objekte löschen	Den Zustand der E-Mail vor seiner Infizierung wiederherstellen. Wenn das Virus nicht desinfizierbar ist oder der Versuch der Desinfizierung nicht erfolgreich war, wird das Objekt gelöscht.
Löschen	E-Mail entfernen. In diesem Fall wird die E-Mail nicht an Adressaten weitergegeben. Anstatt von E-Mail wird eine Nachricht über die ausgeführte Aktion an Postprogramm versandt.
In Quarantäne verschieben	Objekt in das spezielle Verzeichnis der Quarantäne verschieben. In diesem Fall wird die E-Mail nicht an Adressaten weitergegeben. Anstatt dessen wird eine Nachricht über die ausgeführte Aktion an das Mail-Programm gesendet.
Überspringen	E-Mail ohne Anwendung jeglicher Aktionen übergeben.

Bei Entdeckung von schädlichen Objekten in der Post werden alle der obengenannten Einstellungen, außer Aktion **Überspringen,** die Ablehnung der E-Mail-Weitergabe zur Folge haben.

Sie können die Zuverlässigkeit des Antivirusschutzes im Vergleich zu der Default-Ebene steigern, indem Sie in der Liste **Nicht geprüfte E-Mails** den Punkt **In Quarantäne verschieben** wählen. Die Dateien mit den verschobenen E-Mails sollen in diesem Fall folglich unter Anwendung von **Dr.Web Scanner** geprüft werden.

Der Schutz vor verdächtigen E-Mails kann nur dann abgeschaltet werden, wenn sich Ihr Rechner zusätzlich unter dem Schutz des permanent laufenden **SpIDer Guard** Wächters befindet.

Nach der Durchführung der vorgeschriebenen Aktion kann der E-Mail-Wächter **SpIDer Mail** standardmäßig eine entsprechende Benachrichtigung im Infobereich von Windows anzeigen. Sie können die Einstellungen für das Anzeigen der Benachrichtigungen auf dem Bildschirm konfigurieren.

Aktionen, die auf E-Mail angewendet werden

In dieser Gruppe der Einstellungen werden zusätzliche Aktionen für E-Mails angegeben, welche durch den E-Mail-Wächter **SpIDer Mail** bearbeitet wurden.

Einstellung	Beschreibung
Den Header 'X-AntiVirus' den Nachrichten hinzufügen	Per Default aktiviert. Bei der Verwendung dieser Einstellung werden die Informationen über die E-Mail-Prüfung sowie die Version von **Dr.Web** in die Überschrift aller durch **SpIDer Mail** bearbeiteten E-Mails eingefügt. Sie können das Format der hinzugefügten Überschrift nicht ändern.
Modifizierte E-Mails auf dem Server löschen	Bei Verwendung dieser Einstellung werden die eingehenden E-Mails, die vom **SpIDer Mail** E-Mail-Wächter gelöscht oder in die Quarantäne verschoben wurden, auf dem Mailserver gelöscht. Dies erfolgt unabhängig von den Einstellungen des Mail-Programms.

Optimierung der Prüfung

Hier können Sie eine Bedingung festlegen, bei der E-Mails, deren Prüfung viel Zeit in Anspruch nimmt, als nicht geprüfte gelten. Dafür aktivieren Sie die Option **Scan-Timeout für E-Mails (Sek.)** und geben Sie die maximale Dauer für die Prüfung einer E-Mail an. Nach Ablauf dieser Zeit wird die Prüfung vom E-Mail-Wächter **SpIDer Mail** abgebrochen.

Archive

Aktivieren Sie die Option **Archive überprüfen**, um E-Mail-Archive durch **SpIDer Mail** scannen zu lassen. Dabei stehen die folgenden Einstellungen zur Verfügung:

- **Maximale Dateigröße bei Entpackung**. Wenn die Archivgröße nach dem Entpacken den festgelegten Wert übersteigt, werden weder Prüfung noch Entpacken vom E-Mail-Wächter **SpIDer Mail** durchgeführt;
- **Maximaler Kompressionsfaktor**. Wenn der Kompressionsfaktor den angegebenen Wert übersteigt, werden kein Entpacken und keine Prüfung vom E-Mail-Wächter **SpIDer Mail** durchgeführt;
- **Maximale Rekursionstiefe**. Wenn die Rekursionstiefe den angegebenen Wert übersteigt, wird die Prüfung nur bis zu angegebener Rekursionstiefe vom E-Mail-Wächter **SpIDer Mail** durchgeführt.

Um einen oder mehrere Optimierungsparameter zu aktivieren, wählen Sie die entsprechenden Häkchen an.

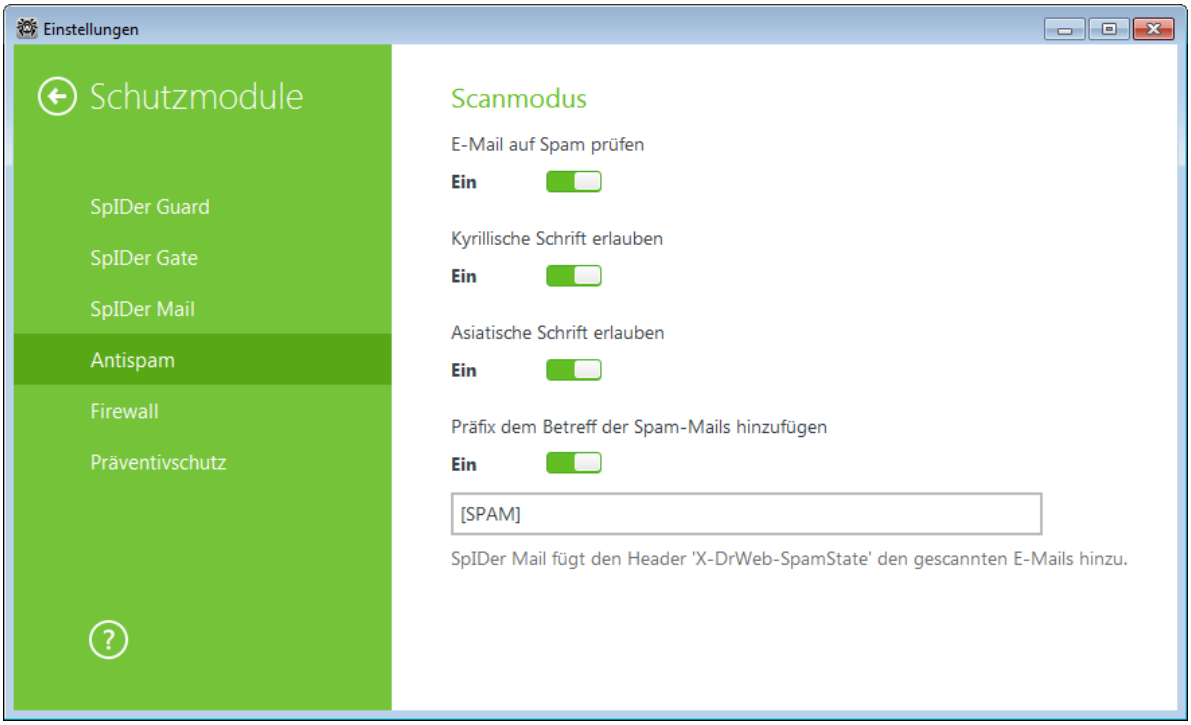
Es gibt keine Einschränkungen für den Parameter, wenn der Parameterwert 0 beträgt.

11.4. Antispam

Dr.Web Antispam

Die Technologie des **Dr.Web** Antispamfilters basiert auf mehreren Tausenden von Regeln, welche bedingt in mehrere Gruppen eingeteilt werden können:

- **Heuristische Analyse –** äußerst komplizierte, hochintellektuelle Technologie der empirischen Auswertung aller E-Mail-Teile: des Betrefffeldes, des E-Mails-Körpers, des Anhanginhalts;
- **Filterung der Gegenwirkung –** basiert auf Erkennung von Ausfluchten, die von Spamern für den Umgang von Antispamfiltern benutzt werden;
- **Analyse auf Basis von HTML-Signaturen –** die Nachrichten, die den HTML-Kode enthalten, werden mit den Mustern der HTML-Signaturen aus der Antispambibliothek verglichen. In Verbindung mit Informationen zu Größen von Abbildungen, die von Spamern in der Regel genutzt werden, schützt ein solcher Vergleich die Benutzer vor Spam-Nachrichten mit Links zu Websites;
- **Semantische Analyse –** Vergleich der Worte und Ausdrücke der Nachrichten mit den für Spam typischen Worten und idiomatischen Wendungen wird mit Hilfe eines speziellen Wörterbuches durchgeführt. Der Analyse werden sowohl sichtbare als auch durch spezielle technische Ausfluchten visuell versteckte Worte, Ausdrücke und Symbole unterzogen;
- **Anti-Scam-Technologie –** zu den Scamming- und Pharming-Nachrichten zählen Nigeria-Scam, Nachrichten über Gewinn bei Lotterien, im Kasino, gefälschte Nachrichten von Banken. Zur deren Filterung wird ein spezielles Modul angewendet;
- **Filterung technischer Spam-Mails** – die sogenannten Bounce-Nachrichten entstehen als Reaktion auf Viren oder als Äußerung von Virenaktivität. Ein spezielles Antispam-Modul markiert solche Nachrichten als unerwünscht.



Bei den Standardeinstellungen werden alle eingehenden E-Mails auf Spam geprüft. Damit die eingehende Korrespondenz nicht geprüft wird, deaktivieren Sie die entsprechende Option.

Sie können auch angeben, welche E-Mails nicht als Spam eingestuft werden sollen sowie auf welche Art die ausgefilterten Nachrichten bezeichnet werden sollen.

Einstellung	Beschreibung
Präfix dem Betreff der Spam-Mails hinzufügen	Per Default aktiviert. Am Anfang des Betreffs einer Spam-E-Mail wird das Präfix „[SPAM]" eingefügt. Diese Einstellung weist dem E-Mail-Wächter **SpIDer Mail** zu, das obengenannte Präfix zum Betreff der als Spam erkannten E-Mails hinzuzufügen. Der Zusatz des Präfixes wird Ihnen helfen, die Filterregeln der als Spam gekennzeichneten E-Mails in solchen E-Mail-Clients zu erstellen, in welchen die Filterung nach E-Mail-Betreff nicht möglich ist (z.B. bei MS Outlook Express).
Black- und Whitelists	Klicken Sie, um die Liste der Absender zu erstellen, deren E-Mails Sie ohne Spamprüfung garantiert freigeben möchten oder garantiert blockieren möchten.

E-Mails mit Spamfilter bearbeiten

Der E-Mail-Wächter **SpIDer Mail** fügt allen geprüften E-Mails die folgenden Überschriften hinzu:

- `X-DrWeb-SpamState: <Wert>`, wobei <*Wert*> weist darauf hin, ob die E-Mail nach Ansicht des E-Mail-Wächters **SpIDer Mail** Spam ist (`Yes`) oder nicht (`No`);
- `X-DrWeb-SpamVersion: <Vesion>`, wobei <Version> – Version der Bibliothek von **Dr.Web Antispam**;
- `X-DrWeb-SpamReason: <Spam-Bewertung>`, wobei <*Spam-Bewertung*> – die Liste mit Bewertungen aufgrund von unterschiedlichen Kriterien für die Zugehörigkeit zu Spam.

Verwenden Sie diese Überschriften und Präfixe im E-Mail-Betreff (wenn das entsprechende Häkchen aktiviert ist), um die Spamfilterung Ihres Mail-Programms einzustellen.

Wenn Sie für den Empfang Ihrer E-Mails IMAP/NNTP-Protokolle benutzen, dann stellen Sie Ihr Mail-Programm so ein, dass die E-Mails vom Mail-Server sofort vollständig geladen werden, ohne dass deren Überschriften vorher angesehen werden können. Dies ist für den korrekten Betrieb des Spamfilters notwendig.

Um die Funktion des Spamfilters zu verbessern, können Sie über die Fehler bei Spamerkennung berichten.

Erkennungsfehler verbessern

1. Sollen Fehler beim Betrieb des Spamfilters auftreten, erstellen Sie eine neue E-Mail und hängen Sie die falsch erkannte Nachricht an. Die Nachrichten im Text der E-Mail werden nicht analysiert.
2. Senden Sie die E-Mail mit Anhang an den Administrator Ihres Antivirus-Netzwerks.

11.5. Dr.Web Firewall

Dr.Web Firewall ist für den Schutz Ihres Rechners vor unbefugtem Zugang von außen bestimmt und beugt den Verlust wichtiger Daten im Netzwerk vor. Diese Komponente gestattet Ihnen die Kontrolle über die Verbindung und Übermittlung von Daten übers Internet sowie die Sperre von verdächtigen Verbindungen auf der Paket- und Anwendungsebenen.

Die **Firewall** bietet Ihnen die folgenden Vorteile:

- Kontrolle und Filterung des kompletten eingehenden und ausgehenden Traffics;
- Kontrolle der Verbindungen auf der Ebene der Anwendungen;
- Filterung der Pakete auf der Netzwerkebene;
- schnelle Umschaltung zwischen Regelsätzen;
- Ereignisse protokollieren.

11.5.1. Dr.Web Firewall Trainingsmodus

Nach der Installation von **Firewall** wird die Weiterbildung des Programms während Ihrer Arbeit am Computer einige Zeit durchgeführt. Beim Entdecken von Verbindungsversuchen zu einem Netzwerk seitens Betriebssystems oder Benutzeranwendungen wird es durch die **Firewall** geprüft, ob Filterregeln für diese Programme festgelegt sind, und wenn es keine Regeln gibt, zeigt eine Warnung an:

Unter einem eingeschränkten Konto (Gast) sendet **Dr.Web Firewall** an Benutzer keine Benachrichtigungen über Verbindungsversuche zum Netzwerk. Die Benachrichtigungen werden unter dem Konto mit Administratorrechten angezeigt, falls eine solche Sitzung zu gleicher Zeit mit der Sitzung vom Gastkonto aktiv ist.

Regeln für Anwendungen

1. Beim Entdecken eines Versuches seitens einer Anwendung, eine Verbindung zum Netzwerk aufzubauen, machen Sie sich mit den folgenden Informationen bekannt:

Feld	Beschreibung
Anwendung	Name des Programms. Überzeugen Sie sich, dass der im Feld **Anwendungspfad** angegebene Pfad dem richtigen Speicherort des Programms entspricht.
Anwendungspfad	Der komplette Pfad der ausführbaren Datei der Anwendung und ihr Name.

Feld	Beschreibung
Digitale Signatur	Die digitale Signatur der Anwendung.
Adresse	Das Protokoll und die Host-Adresse, zu denen versucht wird, eine Verbindung aufzubauen.
Port	Der Port, über welchen der Verbindungsversuch erfolgt.
Richtung	Der Verbindungstyp.

2. Treffen Sie eine Entscheidung über die für diesen Fall passende Operation und wählen Sie eine entsprechende Aktion im unteren Bereich des Fensters aus:
   - Um diese Verbindung einmal zu blockieren, wählen Sie die Aktion **Einmal sperren**.
   - Um der Anwendung diese Verbindung einmal zu erlauben, wählen Sie die Aktion **Einmal erlauben**.
   - um zum Formular zur Regelerzeugung für die Filterung umzuschalten, wählen Sie die Aktion **Regel erstellen.** Es öffnet sich ein Fenster, in welchem Sie entweder eine der voreingestellten Regeln auswählen oder per Hand eine Regel für Anwendungen erstellen können.
3. Klicken Sie auf **OK**. Die **Firewall** führt die von Ihnen angegebene Aktion durch, und das Benachrichtigungsfenster wird geschlossen.

Um Regeln erstellen zu können, benötigen Sie die Administratorrechte.

Falls das Programm, welches eine Verbindung aufzubauen versucht, der **Firewall** bereits bekannt ist (d.h. für das Programm sind Filterregeln angegeben), jedoch durch eine andere unbekannte Anwendung gestartet wird (Parent-Prozess), gibt die **Firewall** eine entsprechende Mitteilung aus.

Regeln für die Parent-Prozesse

1. Wird ein Netzwerkverbindungsversuch seitens der Anwendung entdeckt, die von einem für die **Firewall** unbekannten Programm gestartet wurde, machen Sie sich mit den Informationen über die ausführbare Datei des Parent-Programms vertraut.
2. Wenn Sie eine Entscheidung über die für den Fall passende Aktion getroffen haben, führen Sie eine der folgenden Aktionen durch:
   - Um die Verbindung der Anwendung zum Netzwerk einmal zu blockieren, klicken Sie auf **Sperren**.
   - Um der Anwendung die Verbindung zum Netzwerk einmal zu erlauben, klicken Sie auf **Erlauben**.
   - um eine Regel zu erstellen, klicken Sie auf **Regel erstellen** und im geöffneten Fenster legen Sie die erforderlichen Einstellungen für den Parent-Prozess fest.
3. Klicken Sie auf **OK**. Die **Firewall** führt die von Ihnen angegebene Aktion durch, und das Benachrichtigungsfenster wird geschlossen.

Ebenfalls ist eine Situation möglich, bei welcher eine unbekannte Anwendung durch eine andere unbekannte Anwendung gestartet wird. In solchem Fall wird eine entsprechende Mitteilung angezeigt und bei der Auswahl von **Regel erstellen** wird ein Fenster geöffnet, in dem Sie die Regeln sowohl für die Anwendungen als auch für die Parent-Prozesse erstellen können.

11.5.2. Firewall konfigurieren

Um **Firewall** einstellen zu können, müssen Sie ein entsprechendes Passwort eingeben, wenn im Bereich Einstellungen die Option **Dr.Web Einstellungen mit Passwort schützen** aktiviert ist.

Um die **Firewall** zu starten, führen Sie folgende Schritte durch:

- Auswählen des Funktionsmodus des Programms;
- Erstellen der Liste der autorisierten Anwendungen;
- Einstellungen für bekannte Netzwerke konfigurieren.

Regeln für bekannte Anwendungen werden von der **Firewall** standardmäßig automatisch erstellt. Unabhängig von dem Funktionsmodus erfolgt die Protokollierung der Ereignisse.

Die standardmäßigen Einstellungen sind optimal für die meisten Fälle. Ändern Sie diese nur bei Bedarf.

Die Einstellungsoption **Lokale Verbindungen erlauben** ermöglicht es, allen Anwendungen Verbindungen auf Ihrem Computer ungehindert herzustellen. Auf solche Verbindungen werden keine Regeln angewendet. Deaktivieren Sie dieses Kontrollkästchen, um die Filterregeln unabhängig davon anzuwenden, ob eine Verbindung über das Netzwerk oder innerhalb Ihres Computers hergestellt wird.

Wenn Sie sich als eingeschränkter Benutzer (Gast) angemeldet haben, gibt die **Firewall** eine Meldung über einen Zugriffsfehler aus. Im Menü von **SpIDer Agent** wird die **Firewall** dabei als deaktiviert angezeigt. Die **Firewall** bleibt trotzdem aktiviert und funktioniert gemäß den Standardeinstellungen oder Einstellungen, die früher im Administrator-Modus festgelegt wurden.

Funktionsmodus auswählen

Wählen Sie einen der folgenden Funktionsmodi:

- **Unbekannte Verbindungen erlauben –** Modus, in welchem Zugang zu Netzwerkressourcen den unbekannten Anwendungen gestattet wird;
- **Automatisches Erstellen von Regeln für bekannte Anwendungen –** Modus, in dem Regeln für bekannte Anwendungen automatisch hinzugefügt werden (standardmäßig aktiviert);
- **Interaktiver Modus –** Trainingsmodus, in dem vollständige Kontrolle über die Reaktion der **Firewall** dem Benutzer gewährt wird;
- **Unbekannte Verbindungen sperren –** Modus, in dem alle unbekannten Verbindungen automatisch blockiert werden. Bekannte Verbindungen werden durch die **Firewall** gemäß den festgelegten Filterregeln behandelt.

Automatisches Erstellen von Regeln für bekannte Anwendungen

In diesem Modus werden die Regeln für bekannte Anwendungen automatisch hinzugefügt. Für andere Anwendungen gewährt die **Firewall** Ihnen die Möglichkeit, eine unbekannte Verbindung manuell zu verbieten oder freizugeben sowie eine Regel dafür zu erstellen.

Versucht das Betriebssystem oder eine Benutzeranwendung, den Zugriff auf Netzwerkressourcen zu erhalten, prüft die **Firewall**, ob die Filterregeln für diese Programme erstellt sind. Falls die Regeln fehlen, so erscheint die entsprechende Warnung, in der es Ihnen angeboten wird, entweder eine vorübergehende Lösung zu wählen oder eine Regel zu erstellen, die zur Bearbeitung ähnlicher

Verbindungen im weiteren benutzt wird.

Dieser Modus wird standardmäßig verwendet.

Interaktiver Modus

In diesem Modus wird Ihnen die vollständige Kontrolle über die Reaktion der **Firewall** auf die Erkennung unbekannter Verbindungen gegeben, und somit wird die Ausbildung des Programms während Ihrer Arbeit am PC durchgeführt.

Versucht das Betriebssystem oder eine Benutzeranwendung, den Zugriff auf Netzwerkressourcen zu erhalten, prüft die **Firewall**, ob die Filterregeln für diese Programme erstellt sind. Falls die Regeln fehlen, so erscheint die entsprechende Warnung, in der es Ihnen angeboten wird, entweder eine vorübergehende Lösung zu wählen oder eine Regel zu erstellen, die zur Bearbeitung ähnlicher Verbindungen im weiteren benutzt wird.

Unbekannte Verbindungen erlauben

In diesem Modus werden alle unbekannten Verbindungen zu Netzwerkressourcen, einschließlich Internet, automatisch blockiert.

Bei den Versuchen seitens Betriebssystems oder einer Benutzeranwendung einen Zugang zu Netzwerkressourcen zu erlangen, prüft die **Firewall**, ob Filterregeln für diese Programme festgelegt sind. Wenn es keine Regeln gibt, blockiert die **Firewall** automatisch den Netzwerkzugang und gibt hierbei keine Mitteilungen aus. Wenn die Filterregeln für so eine Verbindung existieren, werden die in den Regeln angegebenen Aktionen durchgeführt.

Erlauben unbekannter Verbindungen

In diesem Modus wird der Zugang zu Netzwerkressourcen, einschließlich Internet, allen unbekannten Anwendungen, für welche keine Filterregeln festgelegt wurden, gewährt. Bei Verbindungsversuchen gibt die **Firewall** keine Mitteilungen aus.

Einstellungen für Anwendungen

Das Filtern auf Anwendungsniveau erlaubt es, den Zugang bestimmter Programme und Prozesse zu Netzwerkressourcen zu kontrollieren sowie den Start anderer Prozesse durch diese Anwendungen zu erlauben bzw. zu verbieten. Sie können die Regeln sowohl für die Benutzer- als auch Systemanwendungen festlegen.

Für jede Anwendung kann jeweils nur ein Regelset für Filterung angegeben werden.

In diesem Abschnitt können Sie die Regelsets für die Filterung gestalten, indem sie neue Regeln erstellen, die bestehenden Regeln bearbeiten und die unnötigen Regeln löschen. De Anwendung wird eindeutig durch den kompletten Pfad der ausführbaren Datei identifiziert. Um den Betriebssystemkern von Microsoft Windows anzugeben (system-Prozess, für den keine entsprechende ausführbare Datei existiert), wird der Name `SYSTEM` verwendet.

Wenn die Datei der Anwendung, für die eine Regel erstellt wurde, geändert wurde (z.B. ein Update installiert wurde), bietet dann die **Firewall** zu bestätigen, dass die Anwendung auf die Netzwerkressourcen zugreifen darf.

Wenn Sie für einen Prozess eine Sperr-Regel erstellt oder den Modus **Unbekannte Verbindungen sperren** ausgewählt haben und später diese Sperr-Regel deaktiviert oder einen anderen Modus ausgewählt haben, wird die aktuelle Sperre verwendet, bis der Prozess wieder versuchen wird, eine Verbindung herzustellen.

Regeln für die vom Rechner entfernten Anwendungen werden nicht automatisch gelöscht. Diese Regeln können nur über den Punkt **Nicht genutzte Regeln entfernen** im Kontextmenü der Liste gelöscht werden.

Im Fenster **Erstelle ein neues Regelset für die Anwendung** (oder **Editiere das Regelset**) können Sie den Zugriff der Anwendung auf die Netzwerkressourcen konfigurieren sowie das Starten anderer Anwendungen erlauben bzw. verbieten.

Um auf dieses Dialogfenster zu gelangen, wählen Sie in den **Firewall-**Einstellungen den Abschnitt **Anwendungen** und klicken Sie auf **Erstellen** oder wählen Sie eine Anwendung aus und klicken Sie auf **Ändern.**

Wenn sich die **Firewall** im Trainingsmodus befindet, können Sie die Regelerstellung unmittelbar aus dem Mitteilungsfenster über eine nicht genehmigte Verbindung aktivieren.

Sonstige Anwendungen starten

Um der Anwendung zu erlauben bzw. zu verbieten, sonstige Anwendungen zu starten, wählen Sie in der Dropdown-Liste **Netzwerkanwendungen starten** eine der nachfolgenden Optionen aus:

- **Erlauben,** um das Starten der Prozesse der Anwendung zu erlauben;
- **Verbieten,** um das Starten der Prozesse der Anwendung zu verbieten;
- **Nicht definiert.** In diesem Fall gelten die Einstellungen des gewählten **Firewall-**Modus für diese Anwendung.

Zugriff auf Netzwerkressourcen

1. Wählen Sie den Zugriffsmodus auf die Netzwerkressourcen:
   - **Alles erlauben –** alle Verbindungen der Anwendung werden erlaubt;
   - **Alles sperren –** alle Verbindungen der Anwendung werden blockiert;
   - **Nicht definiert.** In diesem Fall gelten die Einstellungen des gewählten **Firewall-**Modus für diese Anwendung.
   - **Benutzerdefiniert –** in diesem Modus können Sie ein Set von Regeln erstellen, von welchen die Verbindungen dieser Anwendung erlaubt oder verboten werden.
2. Wenn Sie den Regeltyp **Benutzerdefiniert** für den Zugriff auf die Netzwerkressourcen gewählt haben, wird eine Tabelle mit Informationen zu Regelset für diese Anwendung unten angezeigt.

Parameter	Beschreibung
Aktiviert	Status der Regel.
Aktion	Gibt eine Aktion an, welche von der **Firewall** ausgeführt wird, wenn ein Programm versucht, eine Internetverbindung aufzubauen: • **Pakete sperren –** den Verbindungsversuch blockieren; • **Pakete erlauben –** die Verbindung erlauben.
Regelname	Name der Regel.
Verbindungstyp	Richtung der Verbindung: • **Eingehend –** die Regel wird angewendet, wenn eine Verbindung mit einem Programm auf Ihrem Rechner vom Netzwerk aus initialisiert wird; • **Ausgehend –** die Regel wird angewendet, wenn eine Verbindung von einem Programm auf Ihrem Rechner initialisiert wird; • **Beliebig –** die Regel wird unabhängig von der Richtung der Verbindung angewendet.
Beschreibung	Regelbeschreibung durch Benutzer.

3. Gegebenenfalls können Sie das vorinstallierte Regelset bearbeiten bzw. eigenes Regelset für die Anwendung erstellen.
   - Um eine neue Regel hinzuzufügen, klicken Sie auf **Erstellen**. Die Regel wird am Ende der Liste hinzugefügt.
   - Um eine ausgewählte Regel zu bearbeiten, klicken Sie auf **Ändern**.
   - Um eine Kopie eines bestehenden Regelsets hinzuzufügen, klicken Sie auf **Kopieren**. Die Kopie wird unter dem ausgewählten Regelset hinzugefügt.
   - Um eine ausgewählte Regel zu entfernen, klicken Sie auf **Löschen**.
4. Wenn Sie die Erstellung einer neuen oder die Bearbeitung einer bestehenden Regel gewählt haben, konfigurieren Sie ihre Parameter im angezeigten Fenster.
5. Nach der Bearbeitung klicken Sie auf **OK,** um alle vorgenommenen Änderungen zu speichern, oder auf **Abbrechen,** um sie aufzugeben.

Die Filterregeln regeln das Zusammenwirken des Programms mit bestimmten Hosts im Netzwerk.

Regel erstellen

Geben Sie folgende Parameter der Regel an:

Parameter	Beschreibung
Allgemein	
Regelname	Der Name der zu erstellenden/zu bearbeitenden Regel.
Beschreibung	Kurze Regelbeschreibung.
Aktion	Gibt eine Aktion an, welche von der **Firewall** ausgeführt wird, wenn ein Programm versucht, eine Internetverbindung aufzubauen: • **Pakete sperren –** den Verbindungsversuch blockieren; • **Pakete erlauben –** die Verbindung erlauben.
Status	Der Regelstatus: • **Aktiviert –** die Regel wird angewendet; • **Deaktiviert –** die Regel wird vorübergehend nicht angewendet.
Verbindungstyp	Richtung der Verbindung: • **Eingehend –** die Regel wird angewendet, wenn eine Verbindung mit einem Programm auf Ihrem Rechner vom Netzwerk aus initialisiert wird; • **Ausgehend –** die Regel wird angewendet, wenn eine Verbindung von einem Programm auf Ihrem Rechner initialisiert wird; • **Beliebig –** die Regel wird unabhängig von der Richtung der Verbindung angewendet.
Protokollierung	Modus der Protokollierung: • **Aktiviert –** Ereignisse werden registriert; • **Deaktiviert –** es werden keine Informationen zu Regel gespeichert.
Regeleinstellungen	
Protokoll	Die Protokolle der Netzwerk- bzw. Transportebene, über welche die Verbindung aufgebaut wird. Die folgenden Protokolle der Netzwerkebene werden unterstützt: • **IPv4**; • **IPv6**; • **IP all –** IP-Protokoll beliebiger Version. Die folgenden Protokolle der Transportebene werden unterstützt: • **TCP**; • **UDP**; • **TCP & UDP –** TCP oder UDP Protokoll; • **RAW**.
Lokale Adresse/ entfernte Adresse	IP-Adresse des Remote-Hosts, der in die Verbindung involviert ist. Sie können sowohl eine bestimmte Adresse (**Gleich**), einen Bereich von Adressen (**Im Adressenbereich**) als auch eine Maske des bestimmten Subnetzwerkes (**Maske**) oder die Masken sämtlicher Subnetzwerke, in denen Ihr PC eine Netzwerkadresse besitzt (**MY_NETWORK**) angeben. Um eine Regel für alle Hosts anzugeben, wählen Sie **Beliebig**.
Lokaler Port/ entferner Port	Port, über welchen die Verbindung aufgebaut wird. Sie können sowohl einen bestimmten Port (**Gleich**) als auch einen Bereich von Ports (**Im Adressenbereich**) angeben. Um eine Regel für alle Ports festzusetzen, wählen Sie die Variante **Beliebig**.

Netzwerkschnittstellen

Im Abschnitt **Netzwerkschnittstellen** können Sie angeben, welches Regelset für die Filterung der Pakete verwendet werden soll, die über eine bestimmte Netzwerkschnittstelle übermittelt werden.

Regelset für Netzwerkschnittstelle

1. Um ein Regelset für Filterung von Paketen festzulegen, die über eine bestimmte Netzwerkschnittstelle übertragen werden, wählen Sie im Einstellungsfenster von **Firewall** den Abschnitt **Netzwerkschnittstellen.**
2. Suchen Sie in der Liste nach der gewünschten Schnittstelle und ordnen Sie ihr ein entsprechendes Regelset zu. Wenn das passende Set in der Liste fehlt, erstellen Sie es.
3. Um die Einstellungen zu speichern, klicken Sie auf **OK**.

Um alle verfügbaren Netzwerkschnittstellen anzusehen, klicken Sie auf **Vollständige Liste**. Im geöffneten Fenster können Sie angeben, welche Netzwerkverbindungen in der Tabelle immer anzuzeigen sind. Aktive Netzwerkverbindungen werden in der Tabelle automatisch angezeigt.

Um die Regeln für Netzwerkschnittstellen zu konfigurieren, klicken Sie auf **Konfigurieren**.

Die Filterung auf dem Paketniveau erlaubt die Kontrolle des Netzwerkzugangs unabhängig von den Programmen, welche die Verbindung auslösen. Die Regeln werden zu allen Netzwerkpaketen eines bestimmten Typs angewendet, welche über eine der Netzwerkschnittstellen Ihres PCs übertragen werden.

Im Gegensatz zum Anwendungsfilter bietet dieser Filterungstyp Ihnen allgemeine Kontrollmechanismen.

Die **Firewall** wird mit folgenden voreingestellten Regelsets geliefert:

- **Default Rule –** Regeln, welche die meist gängigen Netzwerkkonfigurationen und verbreiteten Angriffe beschreiben (wird per Default für alle neuen Netzwerkschnittstellen angewendet);
- **Allow All –** alle Pakete werden durchgelassen;
- **Block All –** alle Pakete werden blockiert.

Für das schnelle Umschalten zwischen den Filtermodi können Sie ergänzende Regelsets erstellen.

Regelset für Netzwerkschnittstelle

Um die Parameter des Paketfilters anzugeben, navigieren Sie im Einstellungsfenster der **Firewall** zu **Netzwerkschnittstellen** und klicken Sie auf **Konfigurieren.** In diesem Dialogfenster können Sie:

- Filterregelsätze erstellen, indem Sie neue Regeln erstellen, bestehende Regeln bearbeiten und unnötige Regeln entfernen;
- Zusätzliche Parameter der Filterung angeben.

Regelset erstellen

Um ein Regelset zu erstellen, führen Sie eine der folgenden Schritte durch:

- Um ein Regelset für eine neue Anwendung zu erstellen, klicken Sie auf **Neu**;
- Um ein bestehendes Regelset zu bearbeiten, wählen Sie es in der Liste aus und klicken Sie auf **Editieren**;
- Um eine Kopie des bestehenden Regelsets hinzuzufügen, klicken Sie auf **Kopieren.** Die Kopie wird unter dem ausgewählten Regelset eingefügt;

- Um alle Regeln für ein Programm zu entfernen, wählen Sie das entsprechende Set in der Liste aus und klicken Sie auf **Löschen**.

Zusätzliche Einstellungen

Um zusätzliche Einstellungen für Paketfilterung festzulegen, wählen Sie in der Registerkarte **Einstellungen des Paketfilters** die folgenden Häkchen an:

Kontrollkästchen	Beschreibung
TCP-Filterung des Pakets verwenden	Wählen Sie dieses Häkchen an, um den Zustand der TCP-Verbindung bei der Filterung zu berücksichtigen und nur die Pakete durchzulassen, dessen Inhalte dem aktuellen Zustand entsprechen. In diesem Fall werden alle Pakete, die im Rahmen der Verbindung übermittelt werden, aber nicht der Spezifizierung des Protokolls entsprechen, blockiert. Dieses Mechanismus erlaubt Ihren Rechner vor DoS-Angriffen (Dienstverweigerung), Scannen der Inhalte, Eindringen von Daten und andern böswilligen Operationen besser zu schützen. Ebenfalls wird es empfohlen, dieses Häkchen bei der Verwendung von Protokollen mit komplizierten Algorithmen vom Datentransport (FTP, SIP usw.) anzuwählen. Wählen Sie dieses Häkchen ab, um Pakete ohne Berücksichtigung von TCP-Verbindungen zu filtern.
Fragmentierte IP-Pakete bearbeiten	Wählen Sie dieses Häkchen an, um den Datentransport großer Volumen korrekt zu bearbeiten. Die Größe des Maximalpakets (MTU – Maximum Transmission Unit) kann für verschiedene Netzwerke variieren. Deswegen kann ein Teil der IP-Pakete bei Übermittlung in mehrere Fragmente geteilt werden. Bei der Nutzung dieser Option wird dieselbe Aktion für alle Fragmente angewendet, die durch die Filterregeln für das Hauptpaket (erstes Paket) vorgesehen ist. Wählen Sie dieses Häkchen ab, um Pakete im einzelnen zu bearbeiten.

Regelset

Im Fenster **Regelset editieren** wird eine Liste der Regeln für Paketfilterung, die zu einem bestimmten Set gehören, angezeigt. Sie können die Liste bearbeiten, indem Sie neue Regeln hinzufügen oder die bestehenden Regeln bearbeiten sowie die Reihenfolge deren Anwendung verändern. Die Regeln werden entsprechend der Reihenfolge in der Liste angewendet.

Für jede Regel in der Liste wir folgende Kurzinformation angegeben:

Parameter	Beschreibung
Aktiviert	Status der Regel.
Aktion	Es wird auf die Aktion hingewiesen, die von der **Firewall** bei der Bearbeitung eines Pakets durchgeführt wird: • **Pakete sperren –** Pakete blockieren; • **Pakete erlauben –** Pakete übersenden.
Regelname	Name der Regel.
Richtung	Richtung der Verbindung: • – die Regel wird angewendet, wenn ein Paket aus dem Netzwerk empfangen wird; • – die Regel wird angewendet, wenn ein Paket von Ihrem Computer gesendet wird; • – die Regel wird unabhängig von der Richtung der Verbindung angewendet.

Parameter	Beschreibung
Protokollierung	Der Modus der Registrierung von Ereignissen. Es wird darauf hingewiesen, welche Informationen in dem Protokoll gespeichert werden sollen: • **Header –** nur die Überschriften der Pakete in das Protokoll eintragen; • **Gesamtpaket –** das komplette Paket in dem Protokoll eintragen; • **Deaktiviert –** keine Informationen über die Pakete speichern.
Beschreibung	Kurze Regelbeschreibung.

Regelset bearbeiten

1. Wenn Sie die Erstellung oder Bearbeitung des Regelsets in der Registerkarte **Einstellungen des Paketfilters** gewählt haben, geben Sie im geöffneten Fenster einen Namen des Regelsets an.
2. Um eine Filterregel zu erstellen, verwenden Sie die folgenden Optionen:
   - Um eine neue Regel hinzuzufügen, klicken Sie auf **Erstellen**. Die Regel wird am Anfang der Liste hinzugefügt.
   - Um eine ausgewählte Regel zu bearbeiten, klicken Sie auf **Ändern**.
   - Um eine Kopie eines bestehenden Regelsets hinzuzufügen, klicken Sie auf **Kopieren**. Die Kopie wird vor dem ausgewählten Regelset hinzugefügt.
   - Um eine ausgewählte Regel zu entfernen, klicken Sie auf **Löschen**.
3. Wenn Sie die Erstellung einer neuen oder die Bearbeitung einer bestehenden Regel gewählt haben, konfigurieren Sie ihre Parameter.
4. Benutzen Sie die Pfeilchen rechts von der Liste, um die Reihenfolge der Regelanwendung zu bestimmen. Die Regeln werden nacheinander, entsprechend der Reihenfolge in der Liste, angewendet.
5. Nach der Bearbeitung der Liste klicken Sie auf **OK,** um alle vorgenommenen Änderungen zu speichern, oder auf **Abbrechen,** um sie aufzugeben.

Die Pakete, für die kein Regelset erstellt ist, werden automatisch gesperrt. Davon ausgeschlossen sind die Pakete, die durch die Regeln im Anwendungsfilter erlaubt werden.

Filterregel erstellen

Hinzufügen oder Bearbeiten von Filterregeln

1. Im Fenster zur Bearbeitung des Regelsets für den Paketfilter klicken Sie auf **Neu** oder auf **Editieren.** Es öffnet sich das Fenster zur Erstellung oder Bearbeitung einer Regel für Paketfilterung.
2. Geben Sie folgende Parameter der Regel an:

Parameter	Beschreibung
Regelname	Der Name der zu erstellenden/zu bearbeitenden Regel.
Beschreibung	Kurze Regelbeschreibung.
Aktion	Es wird auf die Aktion hingewiesen, die von der **Firewall** bei der Bearbeitung eines Pakets durchgeführt wird: • **Pakete sperren –** Pakete blockieren; • **Pakete erlauben –** Pakete werden erlaubt.
Richtung	Richtung der Verbindung: • **Eingehend –** die Regel wird angewendet, wenn ein Paket aus dem Netzwerk empfangen wird;

Parameter	Beschreibung
	• **Ausgehend –** die Regel wird angewendet, wenn ein Paket von Ihrem Computer gesendet wird; • **Beliebig –** die Regel wird unabhängig von der Richtung der Verbindung angewendet.
Modus der Protokollierung	Der Modus der Registrierung von Ereignissen. Es wird darauf hingewiesen, welche Informationen in dem Protokoll gespeichert werden sollen: • **Gesamtpaket –** das komplette Paket in dem Protokoll eintragen; • **Header –** nur die Überschriften der Pakete in das Protokoll eintragen; • **Deaktiviert –** keine Informationen über die Pakete speichern.
Kriterium	Filterkriterium. Z. B. Übermittlungs- bzw. Netzwerkprotokoll. Um ein Filterkriterium hinzuzufügen, wählen Sie das benötigte Kriterium in der Dropdown-Liste aus und klicken Sie auf **Hinzufügen.** Sie können beliebige Anzahl der Kriterien hinzufügen. Für einige Überschriften sind zusätzliche Filterkriterien verfügbar.

Fügen Sie keine Filterkriterien hinzu, wird diese Regel alle Pakete (je nach den Einstellungen des Menüfeldes **Aktion**) erlauben bzw. sperren.

Eine Regel für den Paketfilter, die alle Pakete aus dem Subnetzwerk erlaubt, kann beispielsweise wie folgt dargestellt werden:

Wenn Sie in dieser Regel unter der Überschrift IPv4 für die Parameter **Lokale IP-Adresse** und **Remote IP-Adresse** den Wert **Beliebig** eingeben, wird diese Regel für jedes Paket gelten, das den Header IPv4 enthält und von der physischen Adresse eines lokalen Computers verschickt wurde.

11.6. Dr.Web für Outlook

Grundfunktionen der Komponenten

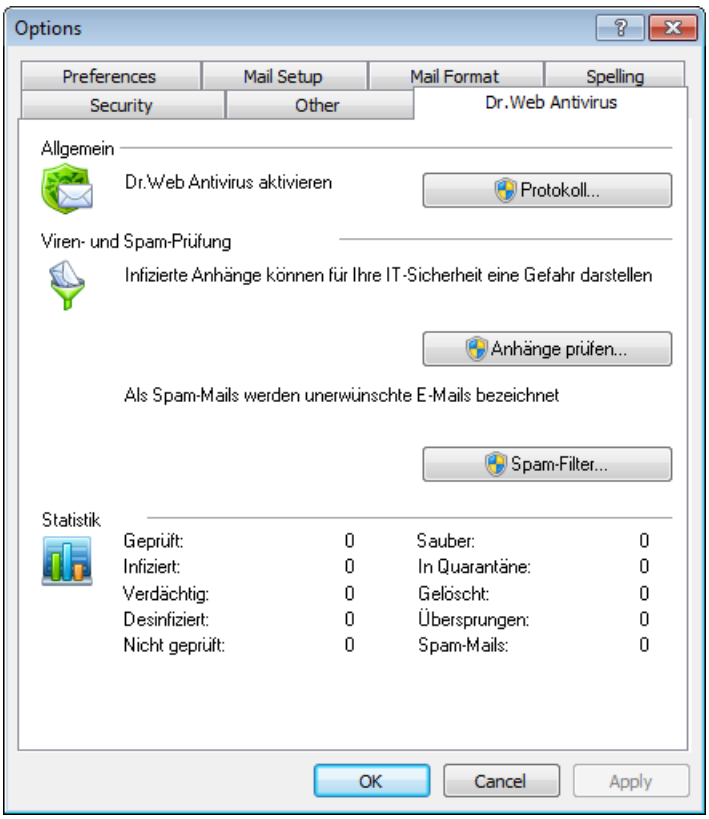
Das Plug-In **Dr.Web für Outlook** hat die folgenden Funktionen:

- Virenprüfung von Anhängen eingehender E-Mails;
- Spam-Prüfung der E-Mails;
- Erkennung und Neutralisierung bösartiger Programme;
- Verwendung der heuristischen Analyse zum zusätzlichen Schutz vor unbekannten Viren.

11.6.1. Dr.Web für Outlook einstellen

Die Einstellung der Programmparameter sowie das Einsehen der Statistiken erfolgt in der E-Mail-Anwendung Microsoft Outlook unter **Extras** →**Optionen** → Registerkarte **Dr.Web Antivirus** (für Microsoft Outlook 2010 gehen Sie auf **Datei** → **Optionen** → **Add-Ins,** wählen Sie das Modul **Dr.Web für Outlook** und klicken Sie auf **Add-Ins Optionen**).

Die zu Einstellungen von Microsoft Outlook gehörende **Dr.Web Antivirus** Registerkarte ist nur zugänglich, wenn der Benutzer die Rechte, die diese Einstellungen ändern lassen, besitzt.



In der Registerkarte **Dr.Web Antivirus** wird der aktuelle Schutzstatus (aktiviert/deaktiviert) angezeigt sowie Zugriff auf folgende Programmoptionen sichergestellt:

- Protokoll – lässt die Registrierung der Programm-Ereignisse einstellen;
- Anhänge prüfen – lässt die E-Mail-Prüfung einstellen sowie Aktionen des Programms für entdeckte schädliche Objekte definieren;
- Spam-Filter – lässt Aktionen des Programms bei Spam-Nachrichten festsetzen sowie White- und Blacklists von E-Mail-Adressen erstellen;
- Statistik – zeigt Angaben zu Objekten, die vom Programm geprüft und bearbeitet wurden.

11.6.2. Erkennung von Bedrohungen

Dr.Web für Outlook verwendet verschiedene Erkennungsmethoden für Viren und andere Bedrohungen. Für erkannte infizierte Objekte werden die durch Benutzer festgelegten Aktionen durchgeführt: sie werden desinfiziert, gelöscht oder in die Quarantäne verschoben, damit sie isoliert werden und somit keinen Schaden Ihrem Rechner zufügen können.

Bösartige Objekte

Dr.Web für Outlook erkennt die folgenden bösartigen Objekte:

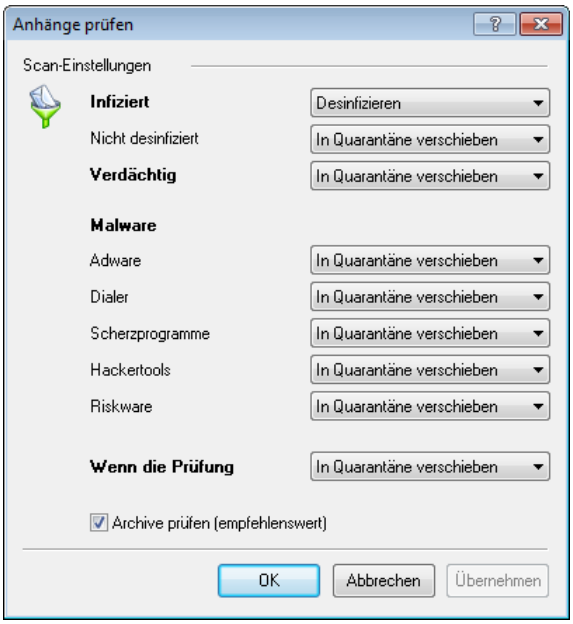
- infizierte Objekte;
- Datei-Bomben und Archivbomben;
- Adware;
- Hacktools;

- Dialer;
- Scherzprogramme;
- Riskware;
- Spyware;
- Trojaner;
- Computerwürmer und Viren.

Aktionen

Dr.Web für Outlook ermöglicht es, Reaktionen beim Fund von infizierten oder verdächtigen Dateien und Schadprogrammen in E-Mail-Anhängen einstellen.

Um die Überprüfung der E-Mail-Anhänge zu konfigurieren und die Aktionen des Programms für die erkannten schädlichen Objekte festzulegen, navigieren Sie in dem E-Mail-Programm Microsoft Outlook zu **Extras** → **Optionen** → Registerkarte **Dr.Web Antivirus** und klicken Sie auf **Anhänge prüfen** (für Microsoft Outlook 2010 gehen Sie auf **Datei** → **Optionen** → **Add-Ins,** wählen Sie das Modul **Dr.Web für Outlook** und klicken Sie auf **Add-Ins Optionen**).



Das Fenster **Anhänge prüfen** ist nur zugänglich, wenn der Benutzer Systemadministratorrechte besitzt.

Wenn Sie unter Windows Vista und neuer auf **Anhänge prüfen** klicken:

- Bei aktivierter UAC: der Administrator erhält eine Aufforderung zur Bestätigung von Programmaktionen. Der Benutzer ohne Administratorrechte erhält eine Aufforderung zur Eingabe von Anmeldedaten des Systemadministrators;
- Bei deaktivierter UAC: der Administrator kann Programmeinstellungen ändern. Der Benutzer erhält keinen Zugriff auf Änderung von Einstellungen.

Im Fenster **Anhänge prüfen** können Sie die Aktionen des Programms für unterschiedliche Kategorien der zu prüfenden Objekte sowie für den Fall, dass Fehler während der Prüfung aufgetreten sind, festsetzen. Sie können auch die Prüfung der Archive aktivieren bzw. deaktivieren.

Zur Definition der Aktionen für entdeckte schädliche Objekte dienen folgende Einstellungen:

- die Dropdown-Liste **Infiziert** setzt die Reaktion auf Entdeckung der Objekte, die mit bekannten und (vermutlich) desinfizierbaren Viren infiziert sind;
- die Dropdown-Liste **Nicht desinfiziert** setzt die Reaktion auf Entdeckung der Objekte, die mit einem bekannten, nicht desinfizierbaren Virus infiziert sind, eingeschlossen der Desinfektionsversuche, die fehlgeschlagen sind;
- die Dropdown-Liste **Verdächtig** setzt die Reaktion auf Entdeckung der Objekte, die mit einem Virus vermutlich infiziert sind (Ergebnis der heuristischen Analyse);
- der Abschnitt **Malware** setzt die Reaktion auf Entdeckung folgender unerwünschter Software fest:
  - Adware,
  - Dialer,
  - Scherzprogramme,
  - Hackertools,
  - Riskware;
- mit der Dropdown-Liste **Wenn die Prüfung fehlgeschlagen ist** lassen sich die Aktionen des Programms für den Fall einstellen, dass die Prüfung eines Anhangs unmöglich ist, z.B. wenn der Anhang eine beschädigte oder mit Passwort geschützte Datei ist.
- mit dem Häkchen bei **Archive prüfen (empfohlen)** lässt sich die Prüfung der als Archiv angehängten Dateien aktivieren oder deaktivieren. Setzen Sie dieses Häkchen zur Aktivierung der Prüfung. Um die Prüfung zu deaktivieren, entfernen Sie das Häkchen.

Die verfügbaren Reaktionen unterscheiden sich je nach dem Typ des Virenereignisses.

Folgende Aktionen können für gefundene Objekte ausgeführt werden:

- **Desinfizieren** (Aktion ist nur für infizierte Objekte zugänglich) – heisst, dass das Programm versucht, das infizierte Objekt zu desinfizieren;
- **Wie für nicht desinfizierte** (Aktion ist nur für infizierte Objekte zugänglich) – heißt, dass eine für nicht desinfizierte Objekte festgelegte Aktion gegen infizierten Anhang verwendet wird;
- **Löschen** – das Objekt wird gelöscht;
- **In Quarantäne verschieben** – das Objekt wird im Quarantäne-Ordner isoliert;
- **Überspringen** – das Objekt wird ohne Änderungen übersprungen.

11.6.3. Spam-Prüfung

Dr.Web für Outlook prüft alle E-Mails mit Hilfe von **Dr.Web Antispam** auf Spam und filtert Nachrichten gemäß den Einstellungen, die vom Benutzer definiert werden.

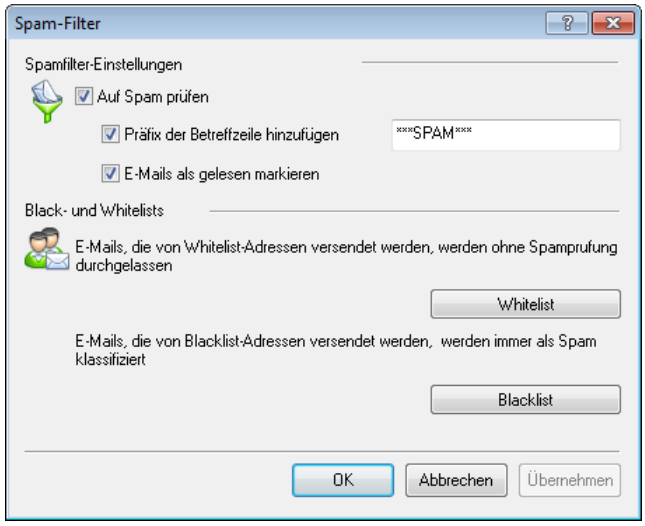
Um die Einstellungen für die Spam-Prüfung der E-Mails zu konfigurieren, navigieren Sie in dem E-Mail-Programm Microsoft Outlook zu **Extras** → **Optionen** → Registerkarte **Dr.Web Antivirus** und klicken Sie auf **Spam-Filter** (für Microsoft Outlook 2010 gehen Sie auf **Datei** → **Optionen** → **Add-Ins,** wählen Sie das Modul **Dr.Web für Outlook** und klicken Sie auf **Add-Ins Optionen**). Das Dialogfenster für die Konfiguration der Einstellungen von Spam-Filter wird geöffnet.

Das Fenster **Spam-Filter** ist nur zugänglich, wenn der Benutzer die Systemadministratorrechte besitzt.

Wenn Sie unter Windows Vista und neuer auf **Spam-Filter** klicken:

- bei aktivierter UAC: der Administrator erhält eine Aufforderung zur Bestätigung von Programmaktionen. Der Benutzer ohne Administratorrechte erhält eine Aufforderung zur Eingabe von Anmeldedaten des Systemadministrators;
- bei deaktivierter UAC: der Administrator kann Programmeinstellungen ändern. Der Benutzer erhält keinen Zugriff auf Änderung von Einstellungen.

Spam-Filter einstellen



Spam-Filter einstellen

Um die Antispamfilterung zu konfigurieren, führen Sie eine der folgenden Aktionen durch:

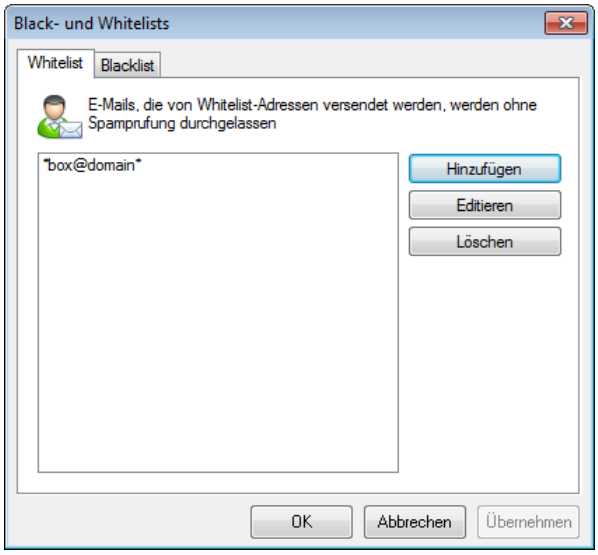
- Aktivieren Sie das Kontrollkästchen **Auf Spam prüfen**, um das Spam-Filter zu aktivieren.
- Wenn Sie einen Text zur Betreffzeile der Nachricht, die als Spam erkannt wurde, hinzufügen wollen, setzen Sie das Häkchen bei **Präfix der Betreffzeile hinzufügen**. Das Feld zur Texteingabe befindet sich rechts vom Kontrollkästchen. Standardmäßig wird das Präfix ***SPAM*** hinzugefügt.
- Geprüfte Nachrichten können in E-Mail-Eigenschaften als gelesen markiert werden. Dafür setzen Sie das Kontrollkästchen **E-Mails als gelesen markieren**. Standardmäßig ist das Kontrollkästchen **E-Mails als gelesen markieren** aktiviert.
- Zur Antispamfilterung können Sie auch White- und Blacklists festlegen.

Wenn manche E-Mails falsch eingestuft wurden, müssen sie an den Administrator Ihres Antivirus-Netzwerks gesendet werden.Alle Nachrichten sind nur im Anhang (nicht im E-Mail-Körper) zu senden.

Black- und Whitelists

Die Black- und Whitelists der E-Mail-Adressen dienen zum Filtern von Nachrichten.

Zum Ansehen und Bearbeiten der Black- oder Whitelist klicken Sie dementsprechend auf **Blacklist** oder **Whitelist** in den Einstellungen des Spam-Filters.



Whitelist oder Blacklist erweitern

1. Klicken Sie auf **Hinzufügen**.
2. Geben Sie die E-Mail-Adresse im entsprechenden Feld ein (s. Eingabemethoden für Whitelist und Blacklist).
3. Klicken Sie auf **OK** im Fenster **Liste bearbeiten**.

E-Mail-Adresse in der Liste ändern

1. Wählen Sie in der Liste die E-Mail-Adresse, die Sie ändern wollen, und klicken Sie auf **Ändern**.
2. Bearbeiten Sie erforderliche Informationen.
3. Klicken Sie auf **OK** im Fenster **Liste bearbeiten**.

E-Mail-Adresse aus der Liste entfernen

1. Wählen Sie in der Liste die E-Mail-Adresse, die Sie entfernen wollen.
2. Klicken Sie auf **Löschen**.

Im Fenster **White- und Blacklists** klicken Sie auf **OK,** um Änderungen zu übernehmen.

Whitelist

Wenn die Absenderadresse zur Whitelist hinzugefügt wird, wird die E-Mail auf Spam nicht geprüft. Wenn aber die Domain-Namen der Empfänger- und Absenderadressen gleich sind und dieser Domain-Name in die Whitelist mit der „*" Maske eingetragen ist, so wird die E-Mail auf Spam geprüft. Eingabemethoden:

- um einen bestimmten Absender zur Liste hinzuzufügen, geben Sie seine komplette E-Mail-Adresse (z.B. `mail@example.net`) an. Alle E-Mails, die von dieser Adresse erhalten werden, werden ohne Spam-Prüfung zugestellt;
- jedes Element der Liste kann nur eine E-Mail-Adresse oder eine Maske enthalten;
- um die E-Mail-Adressen bestimmter Art zur Absenderliste hinzuzufügen, geben Sie eine Maske, die diese Adressen definiert, ein. Die Maske setzt das Template zur Definition des Objektes fest. Sie kann übliche Zeichen, die in E-Mail-Adressen erlaubt sind, sowie das spezielle „*" Zeichen, mit dem eine beliebige (auch leere) Zeichenfolge ersetzt werden kann, beinhalten.

  Beispielsweise sind folgende Varianten möglich:
  - `mailbox@domain.com`
  - `*box@domain.com`
  - `mailbox@dom*`
  - `*box@dom*`

Das „*" Zeichen wird nur am Anfang oder am Ende der E-Mail-Adresse gesetzt.

Das „@" Zeichen ist obligatorisch.

- Um E-Mails von E-Mail-Adressen einer bestimmten Domain garantiert zu erhalten, benutzen Sie das „*" Zeichen anstatt des Benutzernamens. Um alle E-Mails z.B. von Adressaten auf der Domain example.net zu erhalten, geben Sie `*@example.net ein`,
- um E-Mails von E-Mail-Adressen mit einem bestimmten Benutzernamen von einer beliebigen Domain garantiert zu erhalten, benutzen Sie das „*" Zeichen anstatt des Domain-Namens. Um alle E-Mails z.B. von Adressaten mit dem Namen des E-Mail-Postfaches „mustermann" zu erhalten, geben Sie `mustermann@*` ein.

Blacklist

Wenn die Absenderadresse zur Blacklist hinzugefügt wird, wird die E-Mail ohne zusätzliche Analyse als Spam eingestuft. Eingabemethoden:

- um einen bestimmten Absender zur Liste hinzuzufügen, geben Sie seine komplette E-Mail-Adresse (z.B. `spam@spam.de`) an. Alle E-Mails, die von dieser Adresse erhalten werden, werden automatisch als Spam eingestuft;
- jedes Element der Liste kann nur eine E-Mail-Adresse oder eine Maske enthalten;
- um die E-Mail-Adressen bestimmter Art zur Absenderliste hinzuzufügen, geben Sie eine Maske, die diese Adressen definiert, ein. Die Maske setzt das Template zur Definition des Objektes fest. Sie kann übliche Zeichen, die in E-Mail-Adressen erlaubt sind, sowie das spezielle „*" Zeichen, mit dem eine beliebige (auch leere) Zeichenfolge ersetzt werden kann, beinhalten.
- Um E-Mails von E-Mail-Adressen einer bestimmten Domain als Spam garantiert zu markieren, benutzen Sie das „*" Zeichen anstatt des Benutzernamens. Um alle E-Mails z.B. von Adressaten auf der Domain spam.de als Spam zu markieren, geben Sie `*@spam.de` ein.
- Um E-Mails von E-Mail-Adressen mit einem bestimmten Benutzernamen von einer beliebigen Domain als Spam garantiert zu markieren, benutzen Sie das „*" Zeichen anstatt des Domain-Namens. Um alle E-Mails z.B. von Adressaten mit dem Namen des E-Mail-Postfaches „mustermann" als Spam zu markieren, geben Sie `mustermann@* ein`.
- die E-Mail-Adressen auf der Domain des Empfängers werden nicht bearbeitet. Befindet sich z. B. die E-Mail-Adresse des Empfängers (Ihre E-Mail-Adresse) auf der Domain mail.de, werden die von der Domain mail.de abgeschickten E-Mails von dem Spam-Filter nicht bearbeitet.

11.6.4. Ereignisse protokollieren

Dr.Web für Outlook registriert Fehler und aufgetretene Ereignisse in folgenden Protokolldateien:

- Ereignisprotokoll des Betriebssystems (Event Log);
- Debug-Protokolldatei.

Ereignisprotokoll des Betriebssystems

In dem Ereignisprotokoll (Event Log) werden folgende Informationen protokolliert:

- Meldungen beim Starten und Beenden des Programms;
- Parameter der Programm-Module: Scanner, Engine, Virendatenbanken (Information wird beim Starten des Programms und bei Aktualisierung der Module protokolliert);
- Meldungen beim Virenfund.

Um das Ereignisprotokoll des Betriebssystems einzusehen:

1. Öffnen Sie die **Systemsteuerung.**
2. Wählen Sie **Verwaltung** → **Ereignisanzeige** aus.
3. Im linken Fensterbereich der **Ereignisanzeige** wählen Sie den Menüpunkt **Anwendung** aus. Es öffnet sich die Liste der Ereignisse, die durch Benutzeranwendungen in der Protokolldatei registriert wurden. Als Informationsquelle für **Dr.Web für Outlook** tritt die Anwendung **Dr.Web for Outlook** auf.

Debug-Protokolldatei

In der Debug-Protokolldatei werden folgende Informationen protokolliert:

- Meldungen beim Virenfund;
- Meldungen über Schreib- oder Lesefehler der Dateien, Analysefehler bei Archiven und Dateien, die mit Passwort geschützt sind;
- Parameter der Programm-Module: Scanner, Engine, Virendatenbanken;
- Meldungen über sofortiges Stoppen der Programm-Engine.

Protokollierung der Ereignisse einstellen

1. In der Registerkarte **Dr.Web Antivirus** klicken Sie auf **Protokoll**. Es öffnet sich das Einstellungsfenster.
2. Um Ereignisse maximal detailliert zu protokollieren, aktivieren Sie das Kontrollkästchen **Detailliertes Protokoll führen**. Standardmäßig werden nicht alle Ereignisse protokolliert.

Durch die Führung der Debug-Protokolldatei wird die Geschwindigkeit des Betriebssystems beeinträchtigt. In diesem Zusammenhang ist es empfehlenswert, die detaillierte Protokollierung der Ereignisse nur zu aktivieren, wenn Fehler im Betrieb der Anwendung **Dr.Web für Outlook** auftreten.

3. Klicken Sie auf **OK**, um Änderungen zu speichern.

Das Fenster **Protokoll** ist nur zugänglich, wenn der Benutzer Systemadministratorrechte besitzt.

Wenn Sie unter Windows Vista und neuer auf **Protokoll** klicken:

- bei aktivierter UAC: der Administrator erhält eine Aufforderung zur Bestätigung von Programmaktionen. Der Benutzer ohne Administratorrechte erhält eine Aufforderung zur Eingabe von Anmeldedaten des Systemadministrators;
- bei deaktivierter UAC: der Administrator kann Programmeinstellungen ändern. Der Benutzer erhält keinen Zugriff auf Änderung von Einstellungen.

Protokoll einsehen

Zum Ansehen der Ereignis-Protokolldatei des Programms klicken Sie auf **Im Ordner anzeigen.** Es öffnet sich der Ordner, in dem die Protokolldatei gespeichert wird.

11.6.5. Scanstatistiken

In der E-Mail-Anwendung Microsoft Outlook unter **Extras** → **Optionen** → Registerkarte **Dr.Web Antivirus** (für Microsoft Outlook 2010 gehen Sie auf **Datei** → **Optionen** → **Add-Ins,** wählen Sie das Modul **Dr.Web für Outlook** und klicken Sie auf **Add-Ins Optionen**) befinden sich die statistischen Informationen zu der gesamten Anzahl der vom Programm geprüften und bearbeiteten Objekte.

Die Objekte werden in folgende Kategorien aufgeteilt:

- **Geprüft** – Gesamtanzahl der geprüften E-Mails;
- **Infiziert –** Anzahl der E-Mails, die Viren enthalten;
- **Verdächtig –** Anzahl der E-Mails, die vermutlich mit einem Virus infiziert sind (Ergebnis der heuristischen Analyse);
- **Desinfiziert –** Anzahl der Objekte, die vom Programm erfolgreich desinfiziert wurden;
- **Nicht geprüft –** Anzahl der Objekte, deren Prüfung unmöglich ist oder bei deren Prüfung Fehler aufgetreten sind;
- **Sauber –** Anzahl der E-Mails, die keine schädlichen Objekte enthalten.

Dann wird die Anzahl der Objekte, für die Aktionen durchgeführt wurden, wie folgt angezeigt:

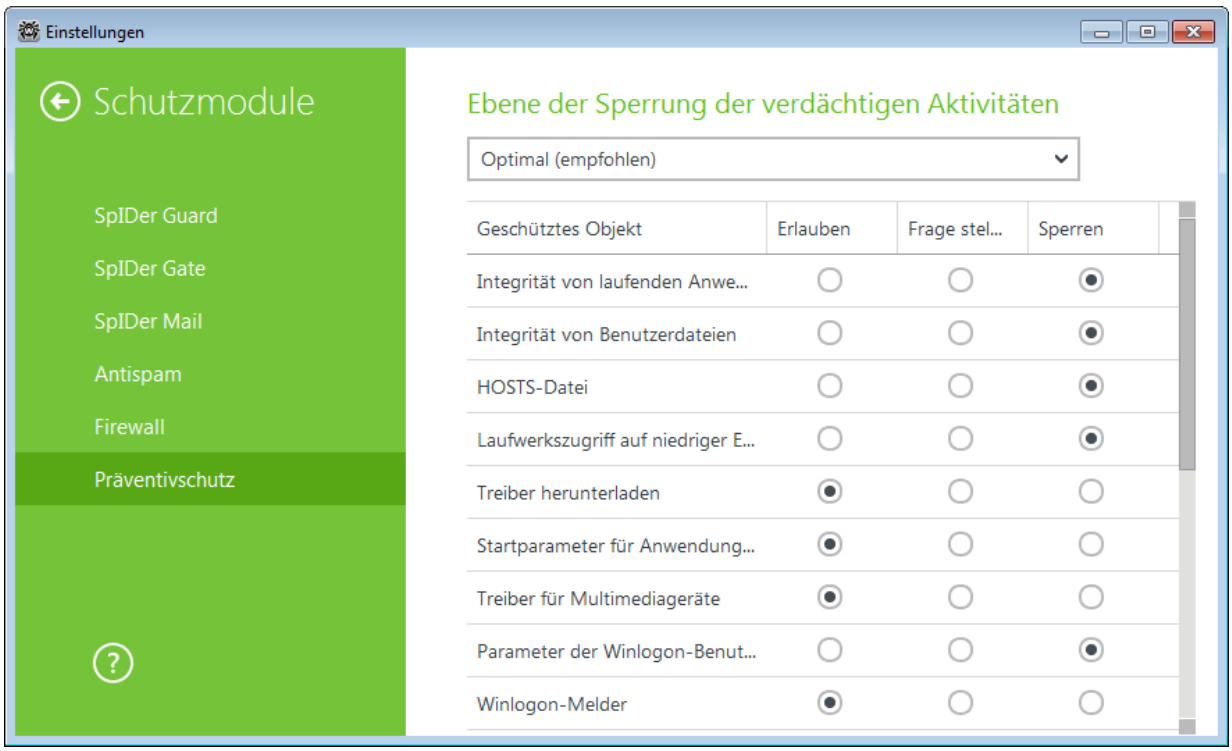
- **In Quarantäne –** Anzahl der Objekte, die in Quarantäne verschoben wurden;
- **Gelöscht –** Anzahl der Objekte, die aus dem System gelöscht wurden;
- **Übersprungen –** Anzahl der Objekte, die ohne Änderungen übersprungen wurden;
- **Spam-Mails –** Anzahl der E-Mails, die als Spam markiert wurden.

Standardgemäß wird die Statistik in der Datei drwebforoutlook.stat gespeichert, die sich im Ordner %USERPROFILE%\DoctorWeb befindet.

Die Statistikdatei drwebforoutlook.stat wird für jeden einzelnen Benutzer des Betriebssystems separat geführt.

11.7. Präventivschutz

In diesem Abschnitt können Sie die Reaktion von **Dr.Web** auf die Aktionen der fremden Programme, die zur Infizierung Ihres Computers führen könnten, festlegen.



Präventivschutz-Niveau

Im Funktionsmodus **Optimal**wird die automatische Änderung von Systemobjekten, deren Modifikation eindeutig auf einen Versuch der Betriebssystemschädigung hindeutet, durch **Dr.Web** verboten. Ebenso wird der Low-Level-Zugriff auf das Laufwerk sowie die Modifizierung der HOSTS-Datei verboten.

Bei einem erhöhten Infizierungsrisiko können Sie das Schutz-Niveau auf **Medium** erhöhen. In diesem Modus wird zusätzlich der Zugriff auf die kritischen Objekte verboten, die potenziell durch Schadprogramme benutzt werden könnten.

In diesem Schutzmodus können Kompatibilitätskonflikte mit der fremden Software auftreten, die geschützte Verzeichniszweige benutzt.

Wird die vollständige Kontrolle über den Zugriff auf die kritischen Windows-Objekte notwendig, kann das Schutz-Niveau auf **Vergesslich** erhöht werden. In diesem Fall werden Sie über die Möglichkeit der interaktiven Kontrolle über das Laden von Treibern und das automatische Starten von Programmen verfügen.

Im Modus **Benutzerdefiniert** können Sie für jedes Objekt die gewünschte Schutzebene wählen.

Geschütztes Objekt	Beschreibung
Integrität von laufenden Anwendungen	Mit dieser Einstellung können Sie Prozesse verfolgen, die in die gestarteten Anwendungen eindringen und die Sicherheit Ihres Rechners dadurch gefährden können. Prozesse, die den Ausnahmen hinzugefügt werden, werden nicht verfolgt.
Integrität von Benutzerdateien	Mit dieser Einstellung können Sie Prozesse verfolgen, welche die Benutzerdateien nach dem bekannten Algorithmus modifizieren. Der Algorithmus weist darauf hin, dass diese Prozesse die Sicherheit des Rechners gefährden. Die Prozesse, die den Ausnahmen hinzugefügt werden, werden nicht verfolgt.

Geschütztes Objekt	Beschreibung
HOSTS-Datei	Die HOSTS-Datei wird von dem Betriebssystem für den vereinfachten Zugang zum Internet benutzt. Änderungen dieser Datei können Ergebnisse der Aktivitäten von Viren bzw. eines anderen Schadprogramms darstellen.
Laufwerkszugriff auf niedriger Ebene	Diese Einstellung erlaubt es, den Anwendungen die Speicherung auf der Festplatte sektorweise zu verbieten, ohne das Dateisystem abzurufen.
Treiber herunterladen	Diese Einstellung erlaubt es, den Anwendungen das Herunterladen neuer bzw. unbekannter Treiber zu verbieten.
Kritische Windows-Bereiche	Die übrigen Einstellungen erlauben es, die Verzeichniszweige vor Modifizierung zu schützen (sowohl im Systemprofil als auch in allen Benutzerprofilen). Zugriff auf Image File Execution Options: • Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options Zugriff auf User Drivers: • Software\Microsoft\Windows NT\CurrentVersion\Drivers32 • Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers Parameter der Winlogon-Benutzeroberfläche: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Winlogon-Benachrichtigungsdienste: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify Autostart der Windows-Oberfläche: • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Dateiverknüpfungen ausführbarer Dateien: • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (Schlüssel) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (Schlüssel) Richtlinien für Softwareeinschränkungen (SRP): • Software\Policies\Microsoft\Windows\Safer Plug-ins für Internet Explorer (BHO): • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Autostart der Programme: • Software\Microsoft\Windows\CurrentVersion\Run • Software\Microsoft\Windows\CurrentVersion\RunOnce • Software\Microsoft\Windows\CurrentVersion\RunOnceEx • Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup • Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup • Software\Microsoft\Windows\CurrentVersion\RunServices • Software\Microsoft\Windows\CurrentVersion\RunServicesOnce Autostart der Richtlinien: • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Konfiguration des abgesicherten Modus: • SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network Session Manager Parameter: • System\ControlSetXXX\Control\Session Manager\SubSystems, Windows

Geschütztes Objekt	Beschreibung
	Systemdienste: • System\CurrentControlXXX\Services

Wenn bei der Installation wichtiger Microsoft-Updates bzw. bei der Installation und Ausführung von Programmen (darunter auch Defragmentierungsprogrammen) Probleme auftreten, deaktivieren Sie vorübergehend den Präventivschutz.

Sie können das Anzeigen von Benachrichtigungen über die Aktionen des Präventivschutzes auf dem Bildschirm konfigurieren.

Anhänge

Anhang A. Befehlszeilenparameter

Befehlszeilenschalter stellen zusätzliche Informationen zum Ausführen der Programme bereit, die durch das Öffnen der jeweiligen ausführbaren Datei gestartet werden können. Zu diesen Programmen zählen **Dr.Web Scanner** und **Konsolen-Scanner**. Mithilfe von Befehlszeilenschaltern können die Parameter festgelegt werden, die in der Konfigurationsdatei nicht enthalten sind. Die Schalter haben Vorrang vor den in der Konfigurationsdatei enthaltenen Parametern.

Befehlszeilenschalter beginnen mit einem Schrägstrich „/" und werden, wie auch andere Befehlszeilenoptionen, durch Leerzeichen getrennt.

Befehlszeilenschalter werden in alphabetischer Reihenfolge aufgeführt.

Befehlszeilenparameter für Scanner und Konsolen-Scanner

`/AA` – Aktionen für erkannte Bedrohungen automatisch anwenden (nur für **Scanner**).

`/AC` – Installationspakete prüfen. Standardmäßig ist diese Option aktiviert.

`/AFS` – den senkrechten Strich bei der Angabe der Rekursionstiefe verwenden. Standardmäßig ist diese Option deaktiviert.

`/AR` – Archive prüfen. Standardmäßig ist diese Option aktiviert.

`/ARC:`*<Kompressionsfaktor>* – maximaler Komprimierungsgrad. Falls es vom Scanner festgestellt wird, dass der Kompressionsfaktor den angegeben Wert übersteigt, wird weder Entpackung noch Prüfung durchgeführt. Standardmäßig gibt es keine Beschränkungen.

`/ARL:`*<Rekursionstiefe>* – maximale Rekursionstiefe des zu prüfenden Archives. Standardmäßig gibt es keine Einschränkungen.

`/ARS:`*<Größe>* – maximale Größe (in KB) des zu prüfenden Archives. Standardmäßig gibt es keine Beschränkungen.

`/ART:`*<Größe>* – Grenzwert (in KB) für die Prüfung des Komprimierungsgrads (minimale Größe einer Datei im Archiv, ab welcher der Kompressionsfaktor geprüft wird). Standardmäßig gibt es keine Beschränkungen.

`/ARX:`*<Größe>* – maximale Größe (in KB) der zu prüfenden Objekte in Archiven. Standardmäßig gibt es keine Beschränkungen.

`/BI` – Information über Virendatenbanken anzeigen. Standardmäßig ist diese Option aktiviert.

`/DR` – Ordner rekursiv scannen (Unterordner scannen). Standardmäßig ist diese Option aktiviert.

`/E:`*<Anzahl_Threads>* – Anzahl der Threads beim Scannen.

`/FAST` – schnelle Prüfung des Systems ausführen (nur für **Scanner**).

`/FL:`*<Dateiname>* – in der Datei angegebene Pfade scannen.

/FM:<*Maske*> – Dateien anhand einer Maske scannen. Standardmäßig werden alle Dateien gescannt.

/FR:<*reg_Ausdruck*> – Dateien nach regulärem Ausdruck scannen. Per Default werden alle Dateien gescannt.

/FULL – vollständige Prüfung aller Festplatten und Wechseldatenträger (einschließlich Bootsektoren) ausführen (nur für **Scanner**).

/FX:<*Maske*> – Dateien, die der Maske entsprechen nicht überprüfen (nur für **Konsolen-Scanner**).

/H oder/? – Kurzhilfe zu Programmbenutzung auf dem Bildschirm anzeigen (nur für **Konsolen-Scanner**).

/HA – heuristische Analyse von Dateien und Suche nach unbekannten Bedrohungen ausführen. Diese Option ist standardmäßig aktiviert.

/KEY:<*Schlüsseldatei*> – Pfad der Schlüsseldatei angeben. Dieser Parameter ist dann erforderlich, wenn sich die Schlüsseldatei und der Scanner in unterschiedlichen Verzeichnissen befinden. Standardmäßig wird die Schlüsseldatei drweb32.key oder eine andere passende Schlüsseldatei im Verzeichnis C:\Program Files\DrWeb\ verwendet.

/LITE – Startprüfung des Systems ausführen. Dabei werden der Hauptspeicher, die Bootsektoren aller Laufwerke gescannt. Es erfolgt auch die Suche nach Rootkits (nur für **Scanner**).

/LN – Dateien scannen, auf die Verknüpfungen zeigen. Die Option ist standardmäßig deaktiviert.

/LS – unter dem Konto LocalSystem scannen. Die Option ist standardmäßig deaktiviert.

/MA – E-Mails scannen. Die Option ist standardmäßig aktiviert.

/MC:<*Anzahl_Versuche*> – maximale Anzahl der Desinfizierungsversuche für eine Datei festlegen. Standardmäßig gibt es keine Beschränkungen.

/NB – keine Backup-Kopien der desinfizierten/gelöschten Dateien erstellen. Die Option ist standardmäßig deaktiviert.

/NI[:X] – genutzte CPU-Leistung (in Prozent). Mit diesem Parameter werden die Größe des für das Scannen zu verwendenden Hauptspeicher und die Systempriorität des Scanprozesses festgelegt.

/NOREBOOT – verhindert den Neustart und das Herunterfahren nach dem Scannen (nur für **Scanner**).

/NT – NTFS-Datenströme scannen. Die Option ist standardmäßig aktiviert.

/OK – komplette Liste der zu scannenden Objekte anzeigen und nicht infizierten Objekte mit Ok markieren. Die Option ist standardmäßig aktiviert.

/P:<*Priorität*> – Priorität der laufenden Aufgabe in der allgemeinen Scan-Aufgaben-Warteschlange:

0 –am niedrigsten.
L – niedrig.
N – normal. Standardpriorität.
H – hoch.
M – maximal.

/PAL:<*Zahl*> – maximale Rekursionstiefe für Packprogramme der ausführbaren Datei. Übersteigt die Rekursionstiefe des zu prüfenden Archives den angegebenen Wert, erfolgt die Überprüfung nur bis zur angegebenen Ebene. Standardmäßig ist der Wert von 1000 voreingestellt.

/QL – Liste sämtlicher Dateien, die auf allen Laufwerken in Quarantäne verschoben wurden, anzeigen (nur für **Konsolen-Scanner**).

/QL:<*Name_des_logischen_Laufwerkes*> – Liste sämtlicher Dateien, die auf dem angegebenen Laufwerk in Quarantäne verschoben wurden, anzeigen (nur für **Konsolen-Scanner**).

/QNA – Pfade mit doppelten Anführungszeichen anzeigen.

/QR[:[d][:p]] – Dateien, die sich in Quarantäne länger als <*p*> (Anzahl) Tage befinden, von dem angegebenen Laufwerk <*d*> *(Name_des_Laufwerks)* löschen. Falls <*d*> und <*p*> nicht angegeben sind, werden alle Dateien in Quarantäne von allen logischen Laufwerken gelöscht (nur für **Konsolen-Scanner**).

/QUIT – den **Scanner** nach der Prüfung beenden (unabhängig davon, ob die Aktionen für entdeckte Bedrohungen ausgeführt wurden) (nur für **Scanner**).

/RA:<*Dateiname*> – Bericht über den Programmbetrieb in der angegebenen Datei fortschreiben. Standardmäßig wird kein Bericht erstellt.

/REP – symbolische Verknüpfungen verfolgen. Die Option ist standardmäßig deaktiviert.

/RA:<*Dateiname*> – Bericht über den Programmbetrieb in die angegebenen Datei schreiben. Standardmäßig wird keine Protokolldatei erstellt.

/RPC:<*Sekunden*> – Timeout (in Sekunden) für die Verbindung mit Scanning Engine. Standardmäßig ist der Wert von 30 Sekunden voreingestellt (nur für **Konsolen-Scanner**).

/RPCD – dynamischen RPC-Identifizierer verwenden (nur für **Konsolen-Scanner**).

/RPCE – dynamische RPC-Zieladresse verwenden (nur für **Konsolen-Scanner**).

/RPCE:<*Zieladresse*> – angegebene RPC-Zieladresse verwenden (nur für **Konsolen-Scanner**).

/RPCH:<*Hostname*> – angegebenen Hostnamen für RPC-Aufrufe verwenden (nur für **Konsolen-Scanner**).

/RPCP:<*Protokoll*> – angegebenes RPC-Protokoll verwenden. Es ist möglich, folgende Protokolle zu verwenden: lpc, np, tcp (nur für **Konsolen-Scanner**).

/SCC – Inhalt der zusammengesetzten Objekte anzeigen. Die Option ist standardmäßig deaktiviert.

/SCN – Namen des Installationspaketes anzeigen. Die Option ist standardmäßig deaktiviert.

/SLS – Protokolle auf dem Bildschirm anzeigen. Die Option ist standardmäßig aktiviert. (nur für **Konsolen-Scanner**).

/SPN – Namen des Packprogramms anzeigen. Die Option ist standardmäßig deaktiviert.

/SPS – Verlauf des Scanvorgangs anzeigen. Die Option ist standardmäßig aktiviert (nur für **Konsolen-Scanner**).

/SST – Scan-Zeit des Objekts anzeigen. Die Option ist standardmäßig deaktiviert.

/TB – Boot-Sektoren und Master Boot Records (MBR) der Festplatte prüfen.

/TM – Suche nach Bedrohungen im Hauptbereich (eingeschlossen vom Windows Systembereich) ausführen.

`/TR` – Systemwiederherstellungspunkte scannen.

`/W:`*<Zahl>* – maximale Scanzeit, in Sekunden. Per Default gibt es keine Beschränkungen.

`/WCL` – Ausgang, der mit drwebwcl kompatibel ist (nur für **Konsolen-Scanner**).

`/X:S[:R]` – nach Beenden des Scanvorgangs den Rechner im angegebenen Modus laufen lassen: Herunterfahren/Neu starten/Energie sparen/Ruhezustand.

Aktionen mit unterschiedlichen Objekten definieren (C – desinfizieren, Q – in Quarantäne verschieben, D – löschen, I – ignorieren, R – benachrichtigen. Die Aktion R ist nur für **Konsolen-Scanner** verfügbar. Die Standardaktion für alle Objekte ist „benachrichtigen" (auch nur für **Konsolen-Scanner**)):

- `/AAD:`*<Aktion>* – Aktionen für Adware (mögliche Aktionen: DQIR)
- `/AAR:`*<Aktion>* – Aktionen für infizierte Archive (mögliche Aktionen: DQIR)
- `/ACN:`*<Aktion>* – Aktionen für infizierte Installationspakete (mögliche Aktionen: DQIR)
- `/ADL:`*<Aktion>* – Aktionen für Dialer (mögliche Aktionen: DQIR)
- `/AHT:`*<Aktion>* – Aktionen für Hackertools (mögliche Aktionen: DQIR)
- `/AIC:`*<Aktion>* – Aktionen für nicht desinfizierbare Dateien (mögliche Aktionen: DQR)
- `/AIN:`*<Aktion>* – Aktionen für infizierte Dateien (mögliche Aktionen: CDQR)
- `/AJK:`*<Aktion>* – Aktionen für Scherzprogramme (mögliche Aktionen: DQIR)
- `/AML:`*<Aktion>* – Aktionen für infizierte E-Mail-Dateien (mögliche Aktionen: QIR)
- `/ARW:`*<Aktion>* – Aktionen für potentiell gefährliche Dateien (mögliche Aktionen: DQIR)
- `/ASU:`*<Aktion>* – Aktionen für verdächtige Dateien (mögliche Aktionen: DQIR)

Einige Schalter können Befehlsmodifizierer haben, mit deren Hilfe der Modus explizit aktiviert oder deaktiviert wird. Zum Beispiel:

`/AC-`	der Modus wird explizit deaktiviert,
`/AC`, `/AC+`	der Modus wird explizit aktiviert.

Diese Möglichkeit kann in dem Fall nützlich sein, wenn der Modus standardmäßig bzw. nach den in der Konfigurationsdatei vorgenommenen Einstellungen aktiviert/deaktiviert ist. Hier finden Sie die Liste der Schalter, die Befehlsmodifizierer haben können:

`/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /TR, /WCL.`

Für den Schalter `/FL` hat der Befehlsmodifizierer „`-`" die folgende Bedeutung: die in der angegebenen Datei aufgelisteten Pfade scannen und die Datei löschen.

Bei den Schaltern `/ARC, /ARL, /ARS, /ART, /ARX, /NI[:X], /PAL, /RPC, /W` bedeutet der Parameterwert „`0`", dass der Parameter ohne Einschränkungen verwendet wird.

Beispiel für die Verwendung von Schaltern beim Start des **Konsolen-Scanners**:

`[`*<Pfad_zum_Programm>*`]dwscancl /AR- /AIN:C /AIC:Q C:\`

alle Dateien, ausgenommen von Archiven, auf dem Laufwerk C scannen, infizierte Dateien desinfizieren, nicht desinfizierbare Dateien in Quarantäne verschieben. Um den **Scanner für Windows** ähnlicherweise zu starten, ist es erforderlich, anstatt von `dwscancl` den Befehlsnamen `dwscanner` anzugeben.

Befehlszeilenparameter für Installationspakete

`/compression` <*Modus*> – Komprimierungsmodus für den Datenverkehr mit dem Zentralschutz-Server. Der Parameter <*Modus*> kann die folgenden Werte haben:

- `yes` – Komprimierung verwenden.
- `no` – keine Komprimierung verwenden.
- `possible` – Komprimierung ist möglich. Entscheidend sind dabei die jeweiligen Einstellungen auf dem Server.

Wenn der Schalter nicht angegeben ist, wird der Wert `possible` standardmäßig verwendet.

`/encryption` <*Modus*> – Verschlüsselungsmodus für den Datenverkehr mit dem Zentralschutz-Server. Der Parameter <*Modus*> kann die folgenden Werte haben:

- `yes` – Verschlüsselung verwenden.
- `no` – keine Verschlüsselung verwenden.
- `possible` – Verschlüsselung ist möglich. Entscheidend sind dabei die jeweiligen Einstellungen auf dem Server.

Wenn der Schalter nicht angegeben ist, wird der Wert `possible` standardmäßig verwendet.

`/excludeFeatures` <*Komponenten*> – hier werden Komponenten aufgelistet, die nicht installiert werden sollen. Als Trennzeichen muss das Kommazeichen „,“ verwendet werden. Folgende Komponenten sind verfügbar:

- `scanner` – **Dr.Web Scanner**,
- `spider-mail` – **SpIDer Mail**,
- `spider-g3` – **SpIDer Guard**,
- `outlook-plugin` – **Dr.Web für Microsoft Outlook**,
- `firewall` – **Dr.Web Firewall**,
- `spider-gate` – **SpIDer Gate**,
- `parental-control` – **Office Control**,
- `antispam-outlook` – **Dr.Web Anti-Spam** für die Komponente **Dr.Web für Microsoft Outlook**,
- `antispam-spidermail` – **Dr.Web Anti-Spam** für die Komponente **SpIDer Mail**.

Komponenten, die explizit nicht angegeben werden, behalten ihren standardmäßigen Installationsstatus.

`/id` <*Workstation_ID*> – ID der Workstation, auf der **Dr.Web Agent** installiert wird.

Eine ID wird zusammen mit einem Passwort (Schalter /pwd) zur manuellen Autorisierung auf dem Server festgelegt. Wenn keine Autorisierungsparameter festgelegt sind, sind dann die Autorisierungseinstellungen auf dem Server entscheidend.

`/installdir` <*Verzeichnis*> – Installationsverzeichnis.

Wenn der Schalter nicht angegeben ist, wird als Installationsverzeichnis das Verzeichnis Program Files

\DrWeb auf dem Systemlaufwerk standardmäßig verwendet.

`/instMode` <*Modus*> – Startmodus für das Installationsprogramm. Der Parameter <*Modus*> kann die folgenden Werte haben:

- `remove` – das installierte Produkt entfernen.

Wenn der Schalter nicht angegeben ist, bestimmt das Installationsprogramm den Startmodus standardmäßig automatisch.

`/lang` <*Sprachcode*> – Sprache des Installationsprogramms und des zu installierenden Produktes. Der Sprachcode soll gemäß der Norm ISO 639-1 angegeben werden.

Wenn der Schalter nicht angegeben ist, wird die Sprache des Systems standardmäßig verwendet.

`/pubkey` <*Pfad*> – der vollständige Pfad zur Datei des öffentlichen Schlüssels.

Wenn kein öffentlicher Schlüssel angegeben ist, verwendet das Installationspogramm bei der lokalen Installation standardmäßig den öffentlichen Schlüssel drwcsd.pub, der sich im Startordner befindet. Wenn der öffentliche Schlüssel in einem anderen Ordner abgespeichert ist, müssen Sie den vollständigen Pfad zum öffentlichen Schlüssel manuell angeben.

Das im Verwaltungscenter erstellte Installationspaket enthält bereits einen öffentlichen Schlüssel. In diesem Fall brauchen Sie keinen zusätzlichen Schalter anzugeben.

`/pwd` <*Passwort*> – Passwort vom **Dr.Web Agent** für den Zugriff auf den Server.

Ein Passwort wird zusammen mit einer ID (Schalter /id) zur manuellen Autorisierung auf dem Server festgelegt. Wenn keine Autorisierungsparameter festgelegt sind, sind dann die Autorisierungseinstellungen auf dem Server entscheidend.

`/regagent` <*Modus*> – bestimmt, ob **Dr.Web Agent** in der Liste der installierten Programme registriert wird. Der Parameter <*Modus*> kann die folgenden Werte haben:

- `yes` – **Dr.Web Agent** wird in der Liste der installierten Programme registriert.
- `no` – **Dr.Web Agent** wird in der Liste der installierten Programme nicht registriert.

Wenn der Schalter nicht angegeben ist, wird der Wert `no` standardmäßig verwendet.

`/retry` <*Anzahl*> – maximale Anzahl der Versuche, den Server über die Versendung von Multicastmeldungen zu finden. Wenn der Server nach der angegebenen Anzahl der Versuche nicht antwortet, wird davon ausgegangen, dass der Server nicht gefunden wurde.

Wenn der Schalter nicht angegeben ist, wird der Standardwert von 3 Versuchen verwendet.

`/server` [<*Protokoll*>/]<*Serveradresse*>[:<*Port*>] – Adresse des Servers, der zur Installation von

Dr.Web Agent verwendet wird und mit dem **Dr.Web Agent** nach der Installation eine Verbindung herstellt.

Wenn der Schalter nicht angegeben ist, wird versucht, den Server über die Versendung von Multicastmeldungen zu finden.

`/silent` <*Modus*> – bestimmt, ob das Installationsprogramm im Hintergrundmodus gestartet wird. Der Parameter <*Modus*> kann die folgenden Werte haben:

- yes – das Installationsprogramm im Hintergrundmodus starten.
- no –das Installationsprogramm im Grafikmodus starten.

Wenn der Schalter nicht angegeben ist, wird der **Dr.Web Agent** im Grafikmodus installiert

`/timeout` <*Zeit*> – Timeoutlimit (in Sekunden) für die Wartung jeder Antwort bei der Suche nach dem Server. Antwortnachrichten werden empfangen, bis das Timeout für die Wartung der Antwort den hier festgelegten Wert überschreitet.

Wenn der Schalter nicht angegeben ist, wird der Standardwert von 3 Sekunden verwendet.

Rückgabecodes

Unten finden Sie mögliche Rückgabecodes und die ihnen entsprechenden Ereignisse:

Rückgabecode	Ereignis
0	Keine Viren oder Bedrohungen wurden gefunden.
1	Bekannte Viren wurden gefunden.
2	Modifikationen der bereits bekannten Viren wurden gefunden.
4	Verdächtige Objekte wurden gefunden.
8	Bekannte Viren wurden in einem Dateiarchiv, einer E-Mail-Archivdatei oder einem Container gefunden.
16	Modifikationen der bereits bekannten Viren wurden in einem Dateiarchiv, einer E-Mail-Archivdatei oder einem Container gefunden.
32	Verdächtige Objekte wurden in einem Dateiarchiv, einer E-Mail-Archivdatei oder einem Container gefunden.
64	Mindestens ein infiziertes Objekt wurde erfolgreich desinfiziert.
128	Mindestens ein infiziertes Objekt wurde entfernt/umbenannt/verschoben.

Der abschließend resultierende Rückgabecode entspricht der Summe der Rückgabecodes der Ereignisse, die beim Scanvorgang vorkamen. Sie können dann die Summe in einzelne Summanden zerlegen, um einzelne eindeutige Rückgabecodes zu ermitteln.

Der Rückgabecode `9 = 1 + 8` bedeutet beispielsweise, dass bekannte Viren, darunter Viren in einem Dateiarchiv, einer E-Mail-Archivdatei oder einem Container, erkannt wurden, dabei keine Desinfizierung durchgeführt wurde, und keine weiteren Bedrohungen beim Scannen gefunden wurden.

Anhang B. Bedrohungen und ihre Neutralisierung

Parallel zur Entwicklung der IT-Technologie und Netzwerklösungen mehren sich auch bösartige Programme, die unerwünscht auf dem Rechner laufen und eventuell dem Benutzer oder System Schaden zufügen. Die ersten Viren erschienen bereits ganz am Anfang der Computer-Ära. Während des Entwicklungsprozesses der Schadprogramme hat sich auch die Antivirensoftware stetig weiterentwickelt. Trotzdem gibt es bis heute keine einheitliche Klassifizierung von Cyber-Bedrohungen. Das liegt in erster Linie daran, dass Virusschreiber immer während neue Technologien und raffinierte Techniken verwenden.

Bösartige Programme können sich über das Internet, lokale Netzwerke, E-Mail-Protokolle und Wechselmedien ausbreiten. Während einige bösartige Programme auf Aktionen eines fahrlässigen und unerfahrenen Benutzers angewiesen sind, können andere Viren ihre Tätigkeiten auf dem infizierten Rechner ganz autark verrichten. Eine andere Gruppe von Schadprogrammen bilden Programme, die für kriminelle Zwecke von Angreifern verwendet werden und sogar gut geschützten Systemen erheblichen Schaden anrichten können.

In diesem Kapitel werden die wichtigsten und am weitaus meist verbreiteten Arten von bösartigen Programmen beleuchtet, vor denen Sicherheitslösungen von **Doctor Web** Ihren Rechner in erster Linie schützen.

Klassifizierung von Bedrohungen

Computerviren

Dieser Typ von bösartigen Programmen zeichnet sich durch die Fähigkeit aus, seinen Code in den ausgeführten Code von anderen Programmen einzubringen. Dieses Eindringen wird als Infizierung bezeichnet. In den meisten Fällen wird die infizierte Datei zum Virenträger, und der eingebrachte Code entspricht nicht unbedingt völlig dem ursprünglichen Code. Die meisten Viren beschädigen oder vernichten Daten. Viren, die in die Dateien des Betriebssystems (normalerweise in ausführbare Dateien und dynamische Bibliotheken) eindringen und beim Zugriff auf das infizierte Programm aktiviert und dann verbreitet werden, sind als Dateiviren bekannt.

Einige bootfähige Viren infizieren nicht Dateien, sondern Starteinträge von Disketten, Festplattenpartitionen und Master Boot Record (MBR) von Festplatten. Diese Viren werden als Bootviren bezeichnet. Sie benötigen ganz wenig Speicherplatz und sind bereit, ihre Funktionen erneut zu realisieren, sobald das System heruntergefahren, neu gestartet oder beendet wird.

Makroviren sind Viren, die Dokumente von Microsoft Office Anwendungen und anderen Programmen, die Makros (werden meistens in Visual Basic geschrieben) verwenden, infizieren können. Makros sind eingebettete Unterprogramme, die in einer der Programmiersprachen kodiert werden. In Microsoft Word können Makros beispielsweise beim Öffnen/Schließen/Speichern eines Dokuments automatisch gestartet werden.

Einige Viren nisten sich im Hauptspeicher des Rechners ein, bleiben dort nach der Ausführung aktiv und können eine Schadensroutine zu späteren Zeitpunkten ausführen. Diese Viren werden als residente bezeichnet.

Die meisten Viren verfügen über eigene Tarnungsmechanismen. Diese Mechanismen werden von Virenautoren ständig raffiniert. Während des Entwicklungsprozesses entwickelen sich auch Techniken zu ihrer Beseitigung.

Verschlüsselte Viren verschlüsseln beispielsweise ihren Code bei jeder Infektion, um ihre Prozesse komplett zu verstecken. Jede Kopie solches Virus enthält nur ein kurzes gemeinsames Fragment, das

trotzdem eventuell zur Signaturendatenbank hinzugefügt werden kann.

Es gibt auch polymorphe Viren, die variabel verschlüsselt sind. Diese Viren ändern bei jeder Infektion ihre Codierung. Dadurch verhindern Sie, dass Virenscanner nach einer speziellen, für den Virus typischen Bytefolge suchen können.

Stealth-Viren – diese Viren versuchen, sich selbst zu verbergen und zu tarnen, indem sie Informationsanforderungen abfangen und falsche Daten zurückgeben. So können sie sich beispielsweise vor einer Prüfung durch einen Virenscanner selbst aus der Datei entfernen und infizieren diese Datei nach der Überprüfung erneut.

Viren können auch nach Sprachen, in denen sie geschrieben sind (i.d.R. sind das Assemblersprache, höhere Programmiersprachen, Skriptsprachen etc.), und nach befallenen Betriebssystemen klassifiziert werden.

Würmer

In letzter Zeit kommen Würmer immer häufiger als Viren und andere bösartige Programme vor. Zwar können solche Programme genauso wie Viren ihre Kopien vervielfältigen, doch sind sie nicht fähig, andere Computerprogramme zu infizieren. Ein Wurm dringt in den Rechner aus dem Netzwerk ein (meistens in E-Mail-Anhängen oder über das Internet) und verschickt seine Kopien an andere Computernetzwerke. Um die Verbreitung zu starten, können Würmer sowohl Benutzeraktionen als auch ein automatisches Verfahren zur Auswahl und Attacke auf Rechner verwenden.

Würmer bestehen nicht unbedingt nur aus einer Datei. Bei vielen Würmern gibt es einen so genannten Infizierungsteil (Shellcode), die in den Arbeitsspeicher geladen wird und lädt unmittelbar den Körper in Form einer ausführbaren Datei. Solange Wurmkörper ins System nicht eingedrungen sind, kann man Würmer durch Neustart loswerden. Wenn sich Würmkörper im System sind, können sie nur von einem Antivirus-Programm entfernt werden.

Aufgrund der intensiven Verbreitung können Würmer Netzwerkeabstürze verursachen, sogar wenn sie das System indirekt beschädigen.

Trojanische Pferde (Trojaner)

Das sind bösartige Programme, die scheinbar eine nützliche Funktion haben, aber im Programm versteckten Code beinhalten, der dem System oder den Nutzern schadet (beschädigt oder löscht Daten, leitet vertrauliche Informationen an Angreifer weiter), oder Unbefugten Zugriff auf den Rechner verschafft.

Trojaner verfügt über die virenähnlichen Tarn- und Schadfunktionen und kann sich sogar als ein Virenmodul erweisen. Hauptsächlich aber verbreiten sich Trojaner als einzelne ausführbare Dateien (sie werden auf Sharehostern hochgeladen, auf Datenträgern gespeichert oder über Netzwerkverbindungen oder E-Mail-Anhänge übertragen), die vom Benutzer oder von einem Systemprozess gestartet werden.

Rootkit

Dabei handelt es sich um die Modifikation einer Gruppe von Programmen mit dem Ziel, Aktivitäten eines Angreifers auf einem System für andere Benutzer des Systems unsichtbar zu machen. Zudem kann ein Rootkit Prozesse anderer Programme, Registrierungsschlüssel, Ordner, Dateien tarnen. Rootkits verbreiten sich als autonome Programme oder als Bestandteile eines anderen bösartigen Programms. Rootkits sind im Allgemeinen Tools, die Angreifer auf dem System installiert, auf das er bereits Zugriff verschafft hat.

Rootkits können je nach Schadensroutine in zwei Gruppen aufgeteilt werden: *User Mode Rootkits (UMR)* – laufen im Benutzermodus, und *Kernel Mode Rootkits (KMR)* laufen im Kernel-Mode. Dadurch

erhält der Angreifer die komplette Kontrolle über einen kompromittierten Rechner. Deswegen ist diese Art von Rootkits schwerer zu entdecken und zu entfernen.

Hacktools

Hacker-Tools sollen Angreifern helfen, Zugriff auf Rechner und Netzwerke zu verschaffen. Am meisten werden Portscanner verwendet, die nach Schwachstellen im Sicherheitssystem des Rechners suchen. Diese Tools können auch von Systemadministratoren benutzt werden, um Sicherheit der bedienten Netzwerke zu überprüfen. Manchmal wird zu Hacktools die Software gezählt, die auf Social Engineering basiert (hierunter versteht man das gezielte Ausnutzen und Provozieren von Benutzerfehlern, um vertrauliche Informationen wie beispielsweise Passwörter zu entwenden).

Spyware

Unter diesem Begriff versteht man Programme, die ohne Genehmigung und Wissen des Benutzers Informationen sammeln und diese dann an Dritte weiterleiten. Diese bösartigen Programme werden häufig auf Bestellung von Werbungsagenturen, Agenturen für Vertriebsmarketing, Spammern, Betrügern, Kriminellen, konkurrierenden Unternehmen usw. entwickelt.

Diese Programme werden unbemerkt zusammen mit nützlicher Software oder beim Aufruf bestimmter Webseiten und Popup-Fenster heruntergeladen und ohne Genehmigung und Wissen des Benutzers installiert. Diese Programme können unter Umständen zum Absturz des Browsers führen oder die Performance des Systems beeinträchtigen.

Adware

Am häufigsten bezeichnet man mit diesem Begriff einen Programmcode, der in eine kostenlose Software eingebettet wird, um dem Benutzer ungewollt Anzeigen zu präsentieren. Solcher Code kann auch geheim von anderen bösartigen Programmen verbreitet werden, um dem Benutzer in seinem Webbrowser Werbung anzuzeigen. Oft verwenden Programme dieses Typs die von Spyware gesammelten Daten.

Scherzprogramme

Darunter fallen bösartige Programme, die dem System keinen direkten Schaden anrichten. Am häufigsten blendet ein solches Programm sinnbefreite Fehlermeldungen ein. Ein Scherzprogramm enthält keinen schädlichen Code, kann aber für Benutzer sehr lästig sein.

Einwahlprogramme (Dialer)

Dialer sind spezielle Computerprogramme, die einen Telefonnummerbereich scannen und dann versuchen, eine Verbindung zu kostenpflichtigen Nummern herzustellen. Provider dieser bösartigen Dialer profitieren von den zusätzlichen Gebühren. Dialer überschreiben die Standardeinstellungen für den Zugriff auf das Internet über die Telefonverbindung ohne Wissen und Einverständnis des Benutzers und veranlassen somit die Einwahl über teure Service-Telefonnummern.

Alle besagten Arten von Programmen sind bösartig, da sie zur Datenbeschädigung oder Entwendung von vertraulichen Informationen des Benutzers verwendet werden können. Programme, die das Eindringen ins System nicht tarnen, Spam-Mails verbreiten und Datenverkehr überwachen werden in der Regel als nicht bösartige angesehen. Unter Umständen können sie aber dem Benutzer oder System Schaden zufügen.

Einige Computerprogramme, die ursprünglich als nützliche Programme konzipiert wurden, können die Systemsicherheit eventuell bedrohen. Das sind nicht nur Programme, die Daten zufällig beschädigen oder löschen können, sondern auch diejenigen Programme, die von Hackern oder anderen Programmen

zur Systembeschädigung missbraucht werden können. Dazu zählen diverse Messaging-Clients, Verwaltungstools, FTP-Server und andere Software.

Unten finden Sie einige Arten von Cyber-Angriffen und Internet-Betrugsmechanismen:

- *Brute-Force-Attacke*. Darunter versteht man das systematische Ausprobieren aller möglichen Passwort-Kombinationen durch eine Software, bis das gesuchte Passwort gefunden ist. Angreifer können bei Brute Force-Attacken auch Wörterbücher einsetzen, um die richtige Passwort-Kombination schneller zu finden.
- *DoS Attacke* (Verweigerung des Dienstes) und *DDoS Attacke* (verteilte Dienstverweigerung). In der Regel verläuft eine DoS -Attacke so, dass während des Angriffs so viel Last auf dem angegriffenen Server erzeugt wird, dass dieser nicht mehr in der Lage ist, seine Aufgaben funktions- und zeitgerecht zu bewältigen, und im schlimmsten Fall zusammenbricht. Bei DDoS-Angriffen wird die Überlastung von einer größeren Anzahl von IP-Adressen verursacht.
- *E-Mail-Bomben* sind die einfachsten Nutzlasttypen. Cyber-Krimineller sendet dabei große Menge von E-Mail-Daten an eine E-Mail-Adresse oder einen Mailserver, um das E-Mail-Programm zu unterbrechen oder einen Mailserver lahmzulegen. Produkte von **Dr.Web** für Mailserver verfügen über spezielle Mechanismen gegen diese Angriffe.
- *Sniffer*. Es handelt sich dabei um ein Werkzeug der Netzwerkanalyse. Ein Sniffer ist eine Software, die den Datenverkehr eines Netzwerks empfangen, aufzeichnen, darstellen und ggf. auswerten kann (auch ohne Wissen und Einverständnis des Benutzers).
- *Spoofing*. Darunter versteht man verschiedene Täuschungsversuche in Computernetzwerken zur Verschleierung der eigenen Identität.
- *Phishing*. Das ist einer der Cyber-Betrugsmechanismen, bei dem persönliche und vertrauliche Daten, wie etwa Kreditkartendaten, Passwörter, entwendet werden. Beim Phishing sendet ein Cyber-Krimineller eine E-Mail an eine große Zahl von Benutzern. Der Benutzer wird mittels dieser E-Mail zu der falschen Webseite geleitet und zur Eingabe seiner Benutzerkontoinformationen aufgefordert. Diese Informationen werden dann gespeichert und zu illegalen Zwecken verwendet.
- *Vishing* (*voice phishing*). Das ist eine Form des Trickbetrugs im Internet. Im Unterschied zu Phishing werden dabei anstelle von E-Mails die sogenannten war diallers (automatisierte Telefonanrufe) und Technologie der VoIP-Telefonie verwendet.

Neutralisierung von Bedrohungen

Es gibt mehrere Methoden zur Virenabwehr. Dank dem komplexen Sicherheitsansatz und flexiblen Einstellungen vereinigen Produkte von **Doctor Web** alle modernen Schutztechniken und bieten somit effektiven Schutz gegen die immer wieder wachsende Cyber-Kriminalität. Die wichtigsten Aktionen zur Neutralisierung der bösartigen Programme sind:

1. *Desinfizieren* ist eine Aktion, die nur bei wesentlichen Bedrohungen (Viren, Würmern und Trojanern) vorgenommen wird. Dabei wird entweder der schädliche Code aus der infizierten Datei entfernt, oder werden funktionsfähige Kopien des bösartigen Programms gelöscht. Außerdem wird es versucht, die Struktur und Funktionsfähigkeit der infizierten Objekte wiederherzustellen. Nicht alle infizierten Dateien können desinfiziert werden, aber gerade Produkte **Doctor Web** bieten die effektivsten Algorithmen zur Desinfektion und zum Reparieren von befallenen Dateien.
2. *In Quarantäne verschieben* ist eine Aktion, bei der ein bösartiges Objekt in einen speziellen Ordner verschoben wird. Damit wird es vom System isoliert und kann kein Schaden zufügen. Diese Aktion muss bei verdächtigen Objekten bevorzugt werden (oder wenn keine Desinfektion möglich ist). Wir empfehlen Ihnen, Kopien dieser Dateien ans **Virenlabor** von **Doctor Web** zu versenden.
3. *Löschen* gilt als die effizienteste Neutralisierungsmethode für alle Computerbedrohungen. Bei dieser Aktion handelt es sich darum, dass das gefährliche Objekt (oder sein Inhalt) endgültig entfernt wird. Denken Sie daran, dass das Löschen manchmal bei Dateien vorgenommen werden kann, für welche die Aktion Desinfizieren gewählt wurde. Das passiert in der Regel dann, wenn eine Datei komplett aus einem schädlichen Code besteht und somit keine nützlichen Informationen enthält. Beim Desinfizieren von Würmern werden beispielsweise alle ihre funktionsfähigen Kopien gelöscht.
4. *Sperren, Umbenennen* sind Aktionen, die ermöglichen, bösartige Programme zu neutralisieren, bei denen aber ihre funktionsfähigen Kopien im Dateisystem erhalten bleiben. Im ersten Fall werden alle Zugriffe auf das bösartige Objekt blockiert. Im zweiten wird die Erweiterung der Datei geändert. Dadurch kann sie nicht ausgeführt werden.

Anhang C. Benennung von Bedrohungen

Bei der Erkennung eines bösartigen Codes wird der Benutzer durch die Komponenten von **Dr.Web** entsprechend benachrichtigt. Dabei wird der Name des bösartigen Programms protokolliert, den Virenforscher von **Doctor Web** diesem Programm vergeben haben. Diese Namen werden nach bestimmten Regeln zusammengestellt und weisen auf die Konstruktion des Virus, Klassen der infizierbaren Objekte, Verbreitungsumgebung (Betriebssysteme und Programmpakete) und andere Besonderheiten hin. Diese Statistiken ermöglichen, Schwachstellen und Sicherheitslücken im geschützten System und in der Software zu finden und zu beseitigen. Unten finden Sie eine kurze Beschreibung der Konventionen, die zur Benennung von Viren verwendet werden. Die aktuellsten und detaillierten Informationen dazu sind immer unter http://vms.drweb.com/classification/ abrufbar.

Es handelt sich dabei um eine rein formale Klassifizierung, da einige Viren gleichzeitig mehrere Eigenschaften besitzen können. Außerdem kann sie aus objektiven Gründen nicht alle Bedrohungen umfassen, da das Spektrum an bösartigen Programmen fast unbeschränkt ist.

Der vollständige Name des Virus besteht aus mehreren durch die Punkte getrennten Elementen. Dabei sind einige am Angang (Präfixe) und am Ende (Suffixe) stehende Elemente sind einheitlich innerhalb dieser Klassifizierung.

Allgemeine Präfixe

Präfixe von Betriebssystemen

Die unten aufgelisteten Präfixe werden verwendet, um Viren zu benennen, die ausführbare Dateien bestimmter Betriebssysteme infizieren:

- `Win` – 16-Bit-Programme unter Windows 3.1;
- `Win95` – 32-Bit-Programme unter Windows 95, Windows 98, Windows M;
- `WinNT` – 32-Bit-Programme unter Windows NT, Windows 2000, Windows XP, Windows Vista;
- `Win32` – 32-Bit-Programme unter Windows 95, Windows 98, Windows Me und Windows NT, Windows 2000, Windows XP, Windows Vista;
- `Win32.NET` – Programme unter Microsoft .NET Framework;
- `OS2` – Programme unter OS/2;
- `Unix` – Programme unter UNIX-basierten Betriebssystemen;
- `Linux` – Programme unter Linux;
- `FreeBSD` – Programme unter FreeBSD;
- `SunOS` – Programme unter SunOS (Solaris);
- `Symbian` – Programme unter Symbian OS (mobil).

Merken Sie bitte, dass einige Viren Programme unter einem Betriebssystem infizieren können, während sie unter einem anderen laufen.

Viren, die Dateien von MS Office infizieren

Präfixe von Viren, die Objekte von MS Office infizieren (angegeben ist die Sprache der Makros, die der jeweilige Virus infiziert):

- `WM` – Word Basic (MS Word 6.0-7.0);
- `XM` – VBA3 (MS Excel 5.0-7.0);

- W97M – VBA5 (MS Word 8.0), VBA6 (MS Word 9.0);
- X97M – VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0);
- A97M – Datenbanken von MS Access'97/2000;
- PP97M – Präsentationsdateien von MS PowerPoint;
- O97M – VBA5 (MS Office'97), VBA6 (MS Office'2000), Virus infiziert Dateien mehrerer Komponenten von MS Office.

Präfixe von Programmiersprachen

Die Präfixgruppe HLL wird verwendet, um Viren zu benennen, die in einer der höheren Programmiersprachen, beispielsweise in C, C++, Pascal, Basic usw., geschrieben sind. Modifizierer weisen dabei auf den Funktionsalgorithmus hin:

- HLLW – Würmer;
- HLLM – E-Mail-Würmer;
- HLLO – Viren, die den Code des befallenen Programms modifizieren können;
- HLLP – parasitäre Viren;
- HLLC – Companion-Viren.

Zu dieser Gruppe gehört auch:

- Java – Viren für die Java Virtual Machine.

Trojanische Pferde

Trojan – ist der Sammelbegriff für verschiedene trojanische Pferde (Trojaner). In einigen Fällen werden Präfixe dieser Gruppe zusammen mit dem Präfix Trojan verwendet.

- PWS – Trojaner, der Passwörter stiehlt;
- Backdoor – RAT-Trojaner (Remotezugriffstrojaner);
- IRC – Trojaner, der Internet Relayed Chat channels verwendet;
- DownLoader – Trojaner, der für den Benutzer unsichtbar bösartige Dateien vom Internet herunterlädt;
- MulDrop – Trojaner, der für den Benutzer unsichtbar Viren herunterlädt, die er in seinem Code enthält;
- Proxy – Trojaner, der Cyber-Kriminellen ermöglicht, den infizierten Rechner zur Navigation im Internet zu verwenden;
- StartPage (auch Seeker) – Trojaner, der Browser-Startseite ändert;
- Click – Trojaner, der Webbrowser-Anfragen auf bestimmte Internet-Ressourcen umleitet;
- KeyLogger – Trojaner, der Maus- und/oder Tastatureingaben aufzeichnen. Auf diese weise können vertrauliche Informationen wie beispielsweise Passwörter entwendet werden;
- AVKill – blockiert oder deinstalliert Antivirenprogramme, Firewalls usw.;
- KillFiles, KillDisk, DiskEraser – löschen bestimmte Gruppen von Dateien (Dateien in einem Verzeichnis oder auf einer Festplatte usw.);
- DelWin – löscht systemkritische (Windows) Dateien;
- FormatC – formatiert das Laufwerk C: (auch FormatAll – formatiert einzelne oder alle Laufwerke);
- KillMBR – beschädigt oder löscht den Inhalt des Master Boot Record (MBR);
- KillMBR – beschädigt oder löscht den Inhalt von CMOS;

Tools zur Ausnutzung von Schwachstellen

- `Exploit` – darunter fallen alle Tools, die bekannte Schwachstellen bestimmter Betriebssysteme oder Anwendungen ausnutzen, um einen bösartigen Code oder Virus ins System einzudringen bzw. den Rechner zu steuern.

Tools für Netzattacken

- `Nuke` – darunter fallen alle Tools, die bekannte Schwachstellen bestimmter Betriebssysteme ausnutzen, um das attackierte System lahmzulegen;
- `DDoS` – Programme dieses Typs realisieren DoS-Attacken auf entfernte Server, um sie lahmzulegen (*Distributed Denial Of Service* – Dienstverweigerung);
- `FDOS` (auch `Flooder`) – *Flooder Denial Of Service* – Programme für Netzattacken, die DoS-Mechanismen verwenden, um Internet-Kanäle lahmzulegen. Im Unterschied zu DoS-Programmen, die mehrere auf verschiedenen Rechnern laufenden Clients verwenden, kann eine FDOS-Programm ganz autark funktionieren.

Script-Viren

Präfixe von Script-Viren, die in verschiedenen Scriptsprachen geschrieben sind:

- `VBS` – Visual Basic Script;
- `JS` – Java Script;
- `Wscript` – Visual Basic Script und/oder Java Script;
- `Perl` – Perl;
- `PHP` – PHP;
- `BAT` – Sprache vom Kommandozeileninterpreter von MS-DOS.

Bösartige Programme

Präfixe von Objekten, die nicht als Viren, sondern als bösartige Programme angesehen werden:

- `Adware` – Adware;
- `Dialer` – Dialer (leitet den Anruf auf eine voreingestellte kostenpflichtige Nummer oder eine kostenpflichtige Webseite um);
- `Joke` – Scherzprogramm;
- `Program` – Riskware (*riskware*);
- `Tool` – Hacktool (*hacktool*).

Sonstiges

Der Präfix `generic` steht nach einem anderen Präfix, der auf die Umgebung oder Programmiersprache hinweist, und dient zur Kennzeichnung eines typischen Beispiels der jeweiligen Gruppe von Viren. Solcher Virus besitzt keine besonderen Eigenschaften (also keine Textzeichenfolgen oder speziellen Effekte), anhand von denen ihm ein Name vergeben werden kann.

Früher wurden solche Viren mit dem Präfix `Silly` gefolgt von verschiedenen Modifizierern gekennzeichnet.

Suffixe

Suffixe werden zur Benennung einiger spezifischer Viren verwendet:

- `generator` – gibt an, dass das Objekt nicht ein Virus, sondern ein Virusgenerator ist;
- `based` – gibt an, das der Virus mithilfe des angegebenen Virusgenerators oder durch die Modifizierung des angegebenen Virus erstellt wurde. In beiden Fällen kennzeichnen die Namen dieses Typs eine Gruppe, zu der Hunderte oder Tausende von Viren gehören können;
- `dropper` – gibt an, dass das Objekt nicht ein Virus, sondern sein Installationsprogramm ist.

© Doctor Web, 2015